AFACEREA EDWARD SNOWDEN

Cele mai șocante dezvăluiri despre spionajul global american

GLENN GREENWALD

„Probabil cel mai influent scriitor despre libertățile civile."
American Prospect

KRONIKA



AFACEREA EDWARD SNOWDEN

Cele mai șocante dezvăluiri despre spionajul global american

GLENN GREENWALD

Glenn Greenwald este autorul de succes al unor cărți importante, printre care, mai recent, *With Liberty and Justice for Some* și *A Tragic Legacy*. Fost avocat și editorialist pentru prestigiosul *The Guardian*, până în octombrie 2013, Greenwald a câștigat numeroase premii pentru comentariile și reportajele sale de investigație, inclusiv premiul top 2013 pentru jurnalism de investigație al Online News Association, Esso Award for Excellence in Reporting (echivalentul brazilian al Premiului Pulitzer) și Pioneer Award pe 2013 din partea Electronic Frontier Foundation. De asemenea, i-a mai fost decernat George Polk Award for National Security Reporting (2013) și a fost desemnat de *Foreign Policy* drept unul dintre primii o sută de gânditori globali. Articolele și reportajele lui Greenwald au apărut în numeroase ziare și reviste de politică, inclusiv în *The New York Times*, *Los Angeles Times* și *The American Conservative*. La începutul anului 2014 a fost cofondator al unui nou outlet media global, *The Intercept*.

AFACEREA EDWARD SNOWDEN

Cele mai șocante dezvăluiri despre spionajul global american

GLENN GREENWALD

LITERA®

No Place to Hide: Edward Snowden, the NSA, and the U.S. Surveillance State
Glenn Greenwald

Ediție publicată prin înțelegere cu Metropolitan Books,
o divizie a Henry Holt and Company, LLC, New York



Editura Litera
O.P. 53; C.P. 212, sector 4, Bucureşti, România
tel.: 021 319 63 90; 031 425 16 19; 0752 548 372
e-mail: comenzi@litera.ro

Ne puteţi vizita pe



Afacerea Edward Snowden.
Cele mai șocante dezvăluiri despre spionajul global american
Glenn Greenwald

Traducere din limba engleză:
Iuliana Daniela Busuioc

Editor: Vidrașcu și fiii
Redactori: Ovidiu Șerban, Andreea Stoica
Copertă: Florentina Tudor
Tehnoredactare și prepress: Anca Suciu

ISBN ePUB: 978-606-741-943-6
ISBN PDF: 978-606-741-944-3
ISBN Print: 978-606-741-534-6

Cuprins

Administrația Statelor Unite a perfecționat o capacitate tehnologică prin care ni se permite să monitorizăm mesajele transmise pe calea aerului... Această capacitate poate fi întoarsă în orice moment împotriva americanilor, și nici un american nu va mai avea intimitate, atât de mare este capacitatea de a monitoriza orice – conversații telefonice, telegrame, nu contează. Nu vei mai avea unde să te ascunzi.

Senatorul Frank Church, președinte al Comisiei din Senat
pentru studierea operațiunilor guvernamentale referitoare
la activitățile serviciilor de informații, 1975

Introducere

În toamna lui 2005, fără să am prea mari așteptări, am decis să creez un blog politic. Nu știam la momentul respectiv cât de mult îmi va schimba viaţa acest lucru, în cele din urmă. Principalul motiv era că deveneam tot mai alarmat de teoriile radicale și extremiste despre putere pe care administraţia americană le adoptase imediat după 11 septembrie 2001 și speram că, scriind despre aceste subiecte, aș putea avea un impact mai mare decât aș fi avut ca avocat de drept constituţional și drept civil, ocupaţie pe care o aveam la momentul respectiv.

La doar șapte săptămâni după ce am început să scriu pe blog, *New York Times* a lansat o bombă: în 2001, scria acesta, administraţia Bush a ordonat în secret Agenţiei de Securitate Naţională (NSA) să supravegheze comunicaţiile electronice ale americanilor fără să solicite în prealabil mandat de la un tribunal penal relevant. La momentul la care a fost dezvăluită, această supraveghere fără mandat era în desfășurare de patru ani și vizase câteva mii de americani.

Subiectul se potrivea perfect cu ceea ce mă interesa pe mine și cu expertiza mea. Administraţia a încercat să justifice programul secret al NSA invocând exact tipul de teorie extremă a puterii executive care mă motivase să încep să scriu: noţiunea că ameninţarea reprezentată de terorism îl investește pe președinte cu o autoritate virtual nelimitată pentru a face orice în scopul de a „menţine naţiunea în siguranţă“, inclusiv autoritatea de a încălca legea. Dezbaterea care a decurs de aici a generat întrebări complexe despre dreptul constituţional și interpretarea statutară, pe care experienţa pe care o aveam m-a făcut dornic să le abordez.

Am petrecut următorii doi ani acoperind fiecare aspect al scandalului privind interceptările fără mandat ale NSA pe

blogul meu și într-o carte din 2006, devenită bestseller. Poziţia mea era simplă: ordonând supravegheri ilegale, președintele a încălcat legea și trebuie tras la răspundere pentru acest lucru. În climatul politic tot mai șovinist și opresiv din America, aceasta s-a dovedit o poziţie extrem de controversată.

Acest context l-a determinat pe Edward Snowden, câţiva ani mai târziu, să mă aleagă ca prima sa persoană de contact pentru a dezvălui încălcările legii făcute de NSA la o scară chiar și mai mare. A spus că el crede că poate conta pe mine ca să înţeleg pericolele supravegherii în masă și caracterul secretos dus la extrem al statului și să nu dau înapoi în faţa presiunii din partea administraţiei și a numeroșilor ei aliaţi din presă și din alte medii.

Volumul remarcabil de documente marcate strict secret pe care Snowden mi l-a transmis, precum și drama care îl înconjura pe Snowden însuși au generat un interes fără precedent în lumea întreagă în ceea ce privește ameninţarea supravegherii electronice în masă și valoarea intimităţii în era digitală. Dar problemele presupuse de aceasta au rămas de-a lungul anilor în mare parte necunoscute.

Există, fără îndoială, multe aspecte ale actualei controverse privind NSA. Tehnologia a permis un tip de supraveghere ubicuă care altădată era doar de domeniul celor mai inventivi scriitori de science-fiction. În plus, veneraţia americană pentru securitate după 11 septembrie a creat un climat deosebit de favorabil abuzurilor de putere. Și, graţie curajului lui Snowden și relativei ușurinţe de a copia informaţia digitală, avem o perspectivă la prima mână fără precedent asupra detaliilor și modului în care operează de fapt sistemul de supraveghere.

Totuși, în privinţa multor aspecte, problemele ridicate de povestea NSA rezonează cu numeroase episoade din trecut. Într-adevăr, opoziţia faţă de invadarea intimităţii de către administraţie a fost un factor major în înfiinţarea Statelor Unite, coloniștii americani protestând faţă de legile care le permiteau oficialilor britanici să percheziţioneze orice casă doreau, după

bunul plac. Coloniștii au convenit că este legitim ca statul să obţină mandate ţintite și specifice pentru a percheziţiona indivizii atunci când există dovezi pentru a putea constitui o cauză probabilă pentru infracţiunile lor. Dar mandatele generale – practica de a face din toţi cetăţenii, fără discriminare, subiect de percheziţie – erau în mod inerent ilegale.

Cel de-al Patrulea Amendament subliniază această idee în legea americană. Limbajul său este clar și succint: „Oamenii au dreptul de a fi în siguranţă ca indivizi, în propriile case, în privinţa documentelor și lucrurilor personale, și nici un mandat nu trebuie emis decât pentru o cauză probabilă, susţinută prin jurământ sau declaraţie și descriind în mod specific locul unde se va căuta și persoana sau lucrurile care vor fi confiscate". Aceasta a avut ca scop, înainte de toate, să abolească pentru totdeauna în America puterea administraţiei de a-și supune cetăţenii la o supraveghere generalizată, fără o suspiciune.

Conflictul privind supravegherea în secolul al XVIII-lea s-a concentrat pe percheziţii, dar cum tehnologia a evoluat, supravegherea a evoluat odată cu ea. La mijlocul secolului al XIX-lea, când extinderea reţelei feroviare a început să permită livrarea corespondenţei mai ieftin și mai rapid, deschiderea corespondenţei pe ascuns de către guvernul britanic[1] a generat un scandal major în Marea Britanie. În primele decenii ale secolului XX, Biroul de Investigaţii[2] american – precursorul FBI-ului de astăzi – folosea interceptările, alături de monitorizarea corespondenţei și informatori, pentru a-i reprima pe cei care se opuneau politicilor administraţiei americane.

Indiferent de tehnicile specifice implicate, supravegherea în masă a avut unele atribute constante de-a lungul istoriei. Iniţial, ţintele supravegherii erau disidenţii și marginalizaţii, lăsându-i pe cei care susţineau guvernul sau erau doar apatici să creadă în mod eronat că sunt imuni. Iar istoria arată că simpla existenţă a unui aparat de supraveghere în masă, indiferent de cum este folosit, este în sine suficientă pentru a înăbuși

disidenţa. Cetăţenii care sunt conștienţi că sunt permanent supravegheaţi devin rapid mai supuși și mai temători.

Investigaţia lui Frank Church de la mijlocul anilor 1970 privind activităţile de spionare ale FBI a descoperit în mod șocant că agenţia etichetase jumătate de milion de cetăţeni americani ca potenţial „subversivi“, în timpul spionării de rutină a persoanelor doar pe baza convingerilor lor politice. (Lista de ţinte a FBI se întindea de la Martin Luther King la John Lennon, de la mișcarea de emancipare a femeilor la Asociaţia anticomunistă John Birch.) Dar flagelul abuzului de supraveghere nu caracterizează doar istoria americană. Dimpotrivă, supravegherea în masă este o tentaţie universală pentru orice putere fără scrupule. Și, de fiecare dată, motivul este același: suprimarea disidenţei și conformarea obligatorie.

Astfel, supravegherea unește guverne care altfel au crezuri politice extrem de diferite. La începutul secolului XX, imperiile britanic și francez[3] au creat departamente specializate de monitorizare pentru a se ocupa de ameninţarea mișcărilor anticolonialiste. După cel de-al Doilea Război Mondial, Ministerul pentru Securitatea Statului din Germania de Est, cunoscut ca STASI, a devenit sinonim cu intruziunea guvernului în viaţa personală. Și mai recent, în timp ce protestele populaţiei din timpul Primăverii Arabe au contestat acapararea puterii de către dictatori, regimurile din Siria, Egipt și Libia au căutat să spioneze folosirea internetului de către disidenţii interni.

Investigaţiile desfășurate de Bloomberg News și *Wall Street Journal* au arătat că, în timp ce aceste dictaturi erau copleșite de protestatari, au cumpărat instrumente de supraveghere de la companii tehnologice occidentale. Regimul din Siria al lui Assad[4] a adus angajaţi de la o companie de supraveghere italiană, Area SpA, cărora li s-a spus că sirienii „au nevoie urgent să urmărească oameni“. În Egipt, poliţia secretă a lui Mubarak[5] a cumpărat tehnologie pentru a sparge codificările Skype și a supraveghea convorbirile activiștilor. Iar în Libia, după cum a relatat *Wall Street Journal,* jurnaliștii și rebelii care au intrat

în centrul de monitorizare în 2011 au găsit „un perete de dispozitive negre de mărimea unui frigider“[6] de la compania de supraveghere franceză Amesys. Echipamentul „inspecta traficul pe internet“ al principalului furnizor de servicii de internet din Libia, „deschizând e-mailuri, spărgând parole, urmărind discuţii online şi cartografiind conexiuni dintre diverşi suspecţi“.

Abilitatea de a supraveghea comunicaţiile persoanelor le dă o putere imensă celor care fac acest lucru. Şi, cu excepţia situaţiei în care o astfel de putere este contrabalansată de un control şi de o responsabilitate riguroase, ea devine aproape sigur ţinta abuzurilor. Să te aştepţi ca administraţia Statelor Unite să opereze o maşinărie de supraveghere masivă într-un secret deplin şi fără să cadă pradă tentaţiilor contravine oricărui exemplu istoric şi tuturor dovezilor privind natura umană.

Într-adevăr, chiar şi înainte de dezvăluirile lui Snowden, devenise evident că a trata Statele Unite cumva ca un caz excepţional în ceea ce priveşte supravegherea este o atitudine extrem de naivă. În 2006, la o audiere în Congres numită „Internetul în China: Un instrument pentru libertate sau suprimare?“[7], vorbitorii au fost de acord în a condamna companiile tehnologice americane pentru că ajută China să suprime disidenţa pe internet. Christopher Smith (membru republican al Camerei Reprezentanţilor din partea statului New Jersey), congresmenul care prezida audierea, a comparat cooperarea Yahoo! cu poliţia secretă chineză cu predarea Annei Frank naziştilor. A fost o tiradă sonoră, o prestaţie tipică pentru situaţiile în care oficialii americani vorbesc despre un regim nealiniat Statelor Unite.

Nici chiar participanţii din Congres nu s-au putut abţine să nu observe că audierea a avut loc la doar două luni după ce *New York Times* dezvăluise vasta supraveghere internă fără mandat desfăşurată de administraţia Bush. În lumina acestor dezvăluiri, denunţarea altor ţări pentru că desfăşoară o supraveghere internă proprie sună mai degrabă fals. Brad Sherman

(membru democrat al Camerei Reprezentanţilor din partea statului California), vorbind după Smith, a remarcat că firmelor tehnologice cărora li se spune să reziste regimului chinez ar trebui să li se spună să fie atente și la propriul guvern. „Altfel“, a avertizat el profetic, „pe când cei din China și-ar putea vedea încălcată intimitatea în cele mai odioase moduri, noi aici în Statele Unite am putea descoperi probabil că unii viitori președinţi, revendicând aceste interpretări foarte largi ale Constituţiei, ne citesc e-mailurile și aș prefera ca acest lucru să nu se întâmple fără un mandat juridic“.

În ultimele decenii, teama de terorism – alimentată de exagerări constante ale ameninţării reale – a fost exploatată de liderii Statelor Unite pentru a justifica o multitudine de politici extremiste. Aceasta a dus la războaie de agresiune, un regim mondial de tortură și de detenţie (chiar asasinare) atât a cetăţenilor străini, cât și americani, fără nici o acuzaţie. Dar sistemul generalizat și secretos al supravegherii în lipsa unor suspiciuni căruia i-a dat naștere ar putea să se dovedească moștenirea sa cea mai durabilă. Aceasta pentru că, în pofida paralelelor istorice, există și o dimensiune cu totul nouă a scandalului privind supravegherea de către NSA: rolul jucat acum de internet în viaţa de zi cu zi.

În special pentru generaţia mai tânără, internetul nu este un domeniu separat, independent, în care se desfășoară câteva activităţi. Nu este pur și simplu poșta sau telefonul nostru. Este mai degrabă epicentrul lumii noastre, locul unde virtual se face totul. Este locul unde se leagă prietenii, unde sunt alese cărţi și filme, unde este organizat activismul politic, unde sunt create și stocate cele mai intime date. Este locul unde ne dezvoltăm și ne exprimăm personalitatea și sinele.

Transformarea acestei reţele într-un sistem de supraveghere în masă are implicaţii diferite de cele ale oricărui alt program de supraveghere anterior. Toate sistemele de spionaj anterioare au fost mai limitate și puteau fi evitate. Să permiţi supravegherii să prindă rădăcini în internet înseamnă să supui

virtual toate formele de interacţiune umană, planificare și chiar gândire unei examinări cuprinzătoare a statului.

Din momentul în care a început să fie folosit la scară largă, internetul a fost văzut de mulţi ca deţinând un potenţial extraordinar: capacitatea de a elibera sute de milioane de persoane prin democratizarea discursului politic și echilibrarea balanţei între cei puternici și cei slabi. Libertatea internetului – posibilitatea de a folosi reţeaua fără constrângeri instituţionale, sociale sau fără controlul statului și fără o teamă permanentă – este centrală în îndeplinirea acestei promisiuni. Convertirea internetului într-un sistem de supraveghere îl privează astfel de potenţialul său central. Mai rău, transformă internetul într-un instrument de represiune, ameninţând să producă arma cea mai opresivă și extremă a intruziunii statului din istorie.

De aceea, dezvăluirile lui Snowden sunt atât de uluitoare și atât de importante. Îndrăznind să expună suprinzătoarele capacităţi de supraveghere ale NSA și chiar și mai surprinzătoarele sale ambiţii, el a clarificat, cu aceste dezvăluiri, că ne aflăm la o răscruce de drumuri istorică. Va fi era digitală un precursor al libertăţii individuale și al libertăţilor politice pe care internetul este singurul capabil să le elibereze? Sau va aduce un sistem de monitorizare și control omniprezent, dincolo de visurile celor mai mari tirani din trecut? Acum, oricare dintre aceste căi este posibilă. Acţiunile noastre vor stabili încotro ne vom îndrepta.

Capitolul 1
Contactul

La 1 decembrie 2012 am fost contactat pentru prima dată de Edward Snowden, deși nu aveam nici o idee la momentul respectiv că era el.

Am primit un e-mail din partea cuiva care își spunea Cincinnatus, o referire la Lucius Quintus Cincinnatus, consulul roman care, în secolul al V-lea î.Hr., a fost numit dictator al Romei pentru a apăra orașul împotriva atacurilor. El a rămas în istorie pentru ceea ce a făcut după ce i-a învins pe inamicii Romei: a renunţat imediat și benevol la putere și s-a întors la viaţa simplă, de la fermă, pe care o ducea înainte. Privit ca un „model de virtute civică“, Cincinnatus a devenit un simbol al folosirii puterii politice în interesul public și al meritului limitării sau chiar renunţării la puterea individuală pentru un bine mai mare.

E-mailul începea așa: „Siguranţa comunicaţiilor persoanelor este foarte importantă pentru mine“ și scopul său declarat era să mă determine să încep să folosesc programul de criptare PGP astfel încât „Cincinnatus“ să poată comunica lucruri despre care, spunea el, este sigur că aș fi interesat. Inventat în 1991, PGP (abreviere de la „pretty good privacy“) a evoluat către un instrument sofisticat pentru a proteja e-mailurile și alte forme de comunicare online faţă de supraveghere și piratare.

Programul „învelește“ fiecare e-mail într-un scut protector, care este un cod compus din sute sau chiar mii de numere și litere, făcând diferenţa între majuscule și minuscule. Cele mai avansate agenţii de informaţii din lume – o clasă care în mod sigur include și Agenţia de Securitate Naţională – are

programe de spargere a parolelor capabile de un miliard de combinaţii pe secundă. Dar codurile de criptare ale PGP sunt atât de lungi și aleatorii încât și cele mai sofisticate programe au nevoie de mai mulţi ani pentru a le sparge. Cei care se tem cel mai mult că au comunicaţiile monitorizate, precum agenţii de informaţii, spionii, activiștii pentru drepturile omului și hackerii, au încredere în această formă de criptare pentru protejarea mesajelor lor.

În e-mailul pe care mi l-a trimis, „Cincinnatus“ afirma că a căutat peste tot după „cheia publică“ de PGP folosită de mine, un set de coduri unic care le permite persoanelor să primească e-mailuri criptate, dar nu a găsit-o. De aici a conchis că nu folosesc programul și mi-a spus: „Acest lucru pune în pericol pe oricine comunică cu tine. Nu susţin că orice comunicare în care ești implicat trebuie criptată, dar ar trebui cel puţin să oferi celor cu care comunici această opţiune“.

„Cincinnatus“ s-a referit apoi la scandalul sexual în care a fost implicat generalul David Petraeus, a cărui relaţie extraconjugală cu jurnalista Paula Broadwell, care i-a pus capăt carierei, a fost descoperită când anchetatorii au găsit e-mailuri schimbate între cei doi pe contul de Google. Dacă Petraeus și-ar fi criptat mesajele înainte de a le încredința Gmail sau de a le stoca, a scris el, atunci anchetatorii nu ar fi putut să le citească. „Criptarea contează și nu este doar pentru spioni și Don Juani.“ Criptarea e-mailurilor, a spus el, „este o măsură de securitate extrem de necesară pentru oricine dorește să comunice cu tine“.

Pentru a mă motiva să îi urmez sfatul, el a adăugat: „Sunt persoane de la care ai vrea să primești informații, dar care nu te vor putea contacta fără să știe că mesajele lor nu pot fi citite în timpul tranzitului“.

Apoi s-a oferit să mă ajute să instalez programul: „Dacă ai nevoie de orice fel de ajutor cu aceasta, anunţă-mă, te rog, sau cere ajutor pe Twitter. Ai mulţi fani experţi în tehnică dispuși să îţi ofere asistenţă imediată“. A semnat: „Mulţumesc. C.“

Intenționam de mult să încep să folosesc un program de codare. Scriam de mulţi ani despre WikiLeaks, avertizori de integritate, hackeri activiști (hacktiviști) cunoscuţi sub numele de Anonymous și subiecte înrudite și am comunicat din când în când cu persoane din interiorul instituţiilor de securitate naţională americane. Multe dintre ele sunt foarte grijulii cu privire la comunicaţiile lor și la prevenirea unei monitorizări nedorite. Dar programul este complicat, mai ales pentru cineva care se pricepe prea puțin la programare și computere, ca mine. Așadar, era unul dintre acele lucruri pe care nu am apucat niciodată să îl fac.

E-mailul lui C. nu m-a făcut să acționez imediat. Am devenit cunoscut pentru că relatez despre subiecte pe care restul presei le ignoră adesea, așa că aud în mod frecvent de la tot felul de persoane cum îmi oferă „un subiect extraordinar" și de obicei se dovedește că nu este nimic. În plus, tot timpul lucrez la mai multe subiecte decât pot gestiona. Așa că am nevoie de ceva concret care să mă determine să renunţ la ce fac pentru a urmări o pistă. În pofida aluziei vagi la „persoanele" de la care „aș vrea să primesc informații", nu era nimic în e-mailul lui C. pe care să îl consider suficient de incitant. L-am citit, dar nu am răspuns.

După trei zile, C. m-a contactat din nou cerându-mi să îi confirm primirea e-mailului anterior. De această dată i-am răspuns rapid. „L-am primit și o să lucrez la asta. Nu am un cod PGP și nu știu cum să fac acest lucru, dar voi încerca să găsesc pe cineva care să mă ajute".

C. a răspuns mai târziu în cursul zilei cu un ghid clar, pas cu pas, despre sistemul PGP: Criptarea pentru Tonți, esenţialul. La sfârșitul instrucţiunilor, care mi s-au părut complexe și confuze, în mare parte din cauza propriei mele ignoranţe, el a spus că acestea sunt doar „noţiunile elementare. Dacă nu găsești pe cineva care să te ghideze în instalare, generare și folosire", a adăugat el, „anunţă-mă, te rog. Îţi pot facilita contactul cu persoane care înţeleg cripto aproape oriunde în lume".

Acest e-mail a avut o încheiere mai marcantă: „Criptografic al tău, Cincinnatus“.

În pofida intenţiilor mele, nu mi-am făcut niciodată timp pentru a lucra la codare. După șapte săptămâni am început să mă simt prost că nu făcusem nimic. Dacă cineva chiar are un subiect important, unul pe care l-aș putea rata doar pentru că nu am reușit să instalez un program pe computer? În afară de asta, criptarea m-ar putea ajuta pe viitor, chiar dacă Cincinnatus se va dovedi că nu are nimic interesant.

La 28 ianuarie 2013 i-am trimis un e-mail lui C. ca să îi spun că voi încerca să găsesc pe cineva care să mă ajute cu criptarea și că sper să fac acest lucru până a doua zi.

C. mi-a răspuns a doua zi: „Este o veste bună! Dacă ai nevoie de orice fel de ajutor sau ai întrebări pe viitor, ești bine-venit să mă contactezi. Te rog să accepţi sincerele mele mulţumiri pentru sprijinirea caracterului privat al comunicaţiilor! Cincinnatus.“

Dar încă o dată nu am făcut nimic, epuizat cum eram la vremea respectivă de alte subiecte și încă nesigur că C. are ceva de spus care să merite. Nu a fost o decizie conștientă să nu fac nimic. Doar că pe lista mea cu lucruri de care trebuie să mă ocup, întotdeauna prea lungă, instalarea unei tehnologii de criptare la cererea acestei persoane necunoscute nu a devenit niciodată prea presantă pentru mine ca să mă opresc din celelalte treburi și să mă concentrez asupra ei.

Astfel, eu și cu C. ne-am trezit într-un cerc vicios. El nu voia să îmi spună nimic clar despre ce are sau cine este și unde a lucrat dacă nu îmi instalam programul de criptare. Dar fără niște detalii care să mă stimuleze, nu era o prioritate să răspund la solicitarea lui și să îmi acord timpul necesar pentru a instala programul.

În faţa lipsei mele de acţiune, C. și-a intensificat eforturile. A realizat o înregistrare video de zece minute intitulată *PGP pentru jurnaliști*. Folosind un program care generează o voce computerizată, înregistrarea video îmi oferea instrucţiuni

într-un mod facil, pas cu pas, despre cum să instalez programul de criptare, completat cu grafice și ilustrații.

Nici de această dată n-am făcut nimic. În acel moment C., așa cum mi-a spus mai târziu, s-a descurajat. „Iată unde am ajuns“, se gândea el, „sunt dispus să îmi risc libertatea, poate chiar și viața, ca să îi înmânez acestui individ mii de documente marcate strict secret de la cea mai secretoasă agenție – o scurgere de informații care va produce zeci, dacă nu sute de știri senzaționale. Și el nici măcar nu se deranjează să instaleze un program de criptare.“

Așa de aproape ajunsesem să dau cu piciorul uneia dintre cele mai mari dezvăluiri despre securitatea națională și cu cele mai multe consecințe din istoria SUA.

Următoarea dată când am auzit despre aceste lucruri a fost zece săptămâni mai târziu. La 18 aprilie am zburat dinspre casa mea din Rio de Janeiro către New York, unde urma să vorbesc despre pericolele secretomaniei guvernamentale și abuzurile împotriva libertăților civile făcute în numele războiului împotriva terorismului.

La aterizarea pe aeroportul JFK, am văzut că am un e-mail de la Laura Poitras, o realizatoare de filme documentare, în care scria: „Există șanse să fii în SUA săptămâna viitoare? Aș vrea să discutăm despre ceva, dar este mai bine să facem asta față în față“.

Iau în serios orice mesaj de la Laura Poitras. Una dintre cele mai hotărâte, mai curajoase și mai independente persoane pe care le-am cunoscut vreodată, ea a făcut film după film în cele mai riscante circumstanțe, fără o echipă sau sprijin din partea unei organizații mass-media, doar cu un buget modest, o cameră de filmat și hotărârea ei. În timpul celor mai grave violențe din timpul Războiului din Irak, ea s-a aventurat în Triunghiul Sunnit pentru a face filmul *My Country, My Country (Țara mea, Țara mea)*, o privire curajoasă asupra vieții sub ocupația SUA, care a fost nominalizat la Oscar.

Pentru următorul ei film, *The Oath (Jurământul)*, Poitras a mers în Yemen, unde a petrecut luni de zile urmărind doi yemeniţi – bodyguardul lui Osama bin Laden și șoferul acestuia. De atunci, Poitras lucrează la un documentar despre supravegherea NSA. Cele trei filme, concepute ca o trilogie despre comportamentul SUA în timpul războiului împotriva terorismului, au făcut din ea o ţintă a hărţuielii autorităţilor guvernamentale de fiecare dată când intră sau iese din ţară.

Prin intermediul Laurei am învăţat o lecţie valoroasă. La momentul la care ne-am întâlnit pentru prima dată, în 2010, ea fusese reţinută pe aeroporturi de Departamentul pentru Securitate Internă de peste 20 de ori în timp ce intra în Statele Unite – fusese interogată, ameninţată, îi fusese confiscat materialul, inclusiv laptopul, aparatele de fotografiat și carneţele de notiţe. Cu toate acestea, ea a decis în mod repetat să nu facă publică hărţuirea neîncetată de teama unor repercusiuni care i-ar fi făcut munca imposibilă. Acest lucru s-a schimbat după un interogatoriu neobișnuit de abuziv pe Aerportul Internaţional Newark Liberty. Laura se săturase. „Devine din ce în ce mai rău, nu mai bine, pentru că tac." Era pregătită ca eu să scriu despre acest lucru.

Articolul pe care l-am publicat în revista politică online *Salon*, detaliind interogatoriile constante la care era supusă Poitras[1], a primit o atenţie substanţială, determinând declaraţii de sprijin și denunţarea hărţuirii. Următoarea dată când Poitras a zburat din Statele Unite după ce am scris articolul nu a mai fost nici un interogatoriu și nu i s-au mai confiscat materialele. În următoarele câteva luni nu a mai existat nici o hărţuire. Pentru prima dată după mulţi ani, Laura putea să călătorească liber.

Lecţia a fost clară pentru mine: oficialilor din cadrul serviciilor de securitate naţională nu le place lumina. Ei acţionează în mod abuziv, ca niște criminali, doar atunci când cred că sunt în siguranţă, în întuneric. Păstrarea secretului este elementul

esenţial al abuzului de putere, am descoperit noi, forţa care îl face posibil. Transparenţa este singurul antidot real.

Pe aeroportul JFK, după ce am citit e-mailul trimis de Laura, i-am răspuns imediat: „De fapt, tocmai am ajuns în SUA în dimineaţa asta... Unde ești?“ Am aranjat o întâlnire pentru ziua următoare, în holul hotelului meu din Yonkers, Marriott, și am găsit locuri la restaurant. La insistenţa Laurei, am schimbat masa de două ori înainte de a începe conversaţia, pentru a fi siguri că nu ne aude nimeni. Laura a trecut apoi la afaceri. Avea „ceva extrem de important și de sensibil“ de discutat, mi-a spus, iar securitatea era vitală.

De vreme ce aveam telefonul cu mine, Laura m-a întrebat dacă i-am scos bateria sau dacă l-am lăsat în camera de hotel. „Sună paranoic“, a spus ea, dar administraţia are capacitatea de a activa telefoanele și laptopurile de la distanţă, ca dispozitive de urmărire. Închiderea telefonului sau a laptopului nu ajută deloc: doar scoaterea bateriei o poate face. Auzisem și înainte asta, de la activiști pentru transparenţă și hackeri, dar am înclinat să îl consider un exces de precauţie. De data aceasta însă, l-am luat în serios pentru că venea de la Laura. După ce am descoperit că bateria telefonului meu nu poate fi scoasă, l-am dus în cameră, după care m-am întors la restaurant.

Abia acum a început Laura să vorbească. Primise o serie de e-mailuri anonime de la cineva care părea onest și serios. Persoana respectivă pretindea că are acces la documente extrem de secrete și incriminatoare despre un program al administraţiei americane de spionare a propriilor cetăţeni și a restului lumii. Era hotărât să îi dea aceste documente și a cerut în mod specific ca ea să lucreze cu mine pentru publicarea și relatarea lor. Nu am făcut nici o legătură la acel moment cu e-mailurile de mult uitate pe care le primisem de la Cincinnatus cu luni înainte. Ele se aflau undeva în mintea mea, dar nu la îndemână.

Laura a scos apoi câteva pagini din geantă cu două dintre e-mailurile trimise de informatorul anonim și le-am citit la masă de la început până la sfârșit. Erau fascinante.

Cel de-al doilea e-mail, trimis la câteva săptămâni după primul, începea: „Încă aici“. Referitor la întrebarea care mă chinuia – când va fi gata să furnizeze documente? – el scrisese „Tot ce pot spune este «curând»“.

După ce îi cerea să scoată mereu bateriile din telefoane înainte de a discuta lucruri sensibile – sau cel puţin să pună telefoanele în frigider, unde capacităţile de supraveghere a lor ar fi împiedicate –, informatorul îi spunea Laurei că ar trebui să lucreze cu mine la aceste documente. După care a ajuns la esenţa a ceea ce el considera că este misiunea sa:

> Şocul acestei perioade inițiale [după prima dezvăluire] va furniza sprijinul necesar pentru construirea unui internet mai egal, dar acesta nu va funcționa în avantajul persoanei obişnuite decât dacă ştiința depăşeşte legea. Înțelegând mecanismele prin care intimitatea noastră este încălcată, putem învinge. Putem garanta pentru toate persoanele protecție egală împotriva verificării excesive prin legi universale, dar numai în cazul în care comunitatea tehnică vrea să înfrunte amenințarea şi să se implice în implementarea unor soluții mult prea complicate. În cele din urmă, trebuie să susținem un principiu prin care singura modalitate ca omul puternic să se bucure de intimitate să fie atunci când aceasta este de acelaşi fel cu cea a omului de rând: una susținută de legile naturii, mai degrabă decât de politicile omului.

„Este real“, am spus atunci când am terminat de citit. „Nu pot să explic exact de ce, dar intuiția îmi spune că e serios, că este exact cine spune că este.“

„Și eu la fel“, a replicat Laura. „Am foarte puţine îndoieli.“

Raţional vorbind, eu și Laura am știut că încrederea noastră în veridicitatea informatorului ar putea fi o greșeală. Nu aveam nici o idee cine îi scria. Putea fi oricine. Putea să fi inventat întreaga poveste. Putea, de asemenea, să fie un fel de complot pus la cale de administraţie pentru a ne prinde în cursă cu o scurgere de informaţii cu consecinţe penale. Sau poate venea

de la cineva care intenţiona să ne prejudicieze credibilitatea oferindu-ne documente false[2] pentru a le publica.

Am discutat toate aceste posibilităţi. Știam că un raport secret al Armatei SUA din 2008 declarase WikiLeaks inamic al statului și propusese modalităţi de „prejudiciere și potenţială distrugere" a organizaţiei. Raportul (care, ironic, a intrat în posesia WikiLeaks) discuta despre posibilitatea de a transmite documente false. Dacă WikiLeaks le publica drept autentice, suferea o lovitură gravă în privința credibilității.

Eu și Laura eram conștienţi de toate capcanele, dar le-am ignorat, bazându-ne în schimb pe intuiţia noastră. Ceva intangibil, dar puternic legat de acele e-mailuri ne-a convins că autorul lor este sincer. A scris convins fiind de pericolele secretului guvernamental și ale spionajului omniprezent: am recunoscut instinctiv patima sa politică. Am simţit o legătură cu corespondentul nostru, cu viziunea lui despre lume și cu sentimentul urgenţei care îl consuma în mod clar.

În ultimii șapte ani am fost mânat de aceeași convingere, scriind aproape zilnic despre tendinţele periculoase ale secretului de stat în SUA, despre teoriile puterii executive radicale, despre abuzurile privind detenţia și supravegherea, militarismul și atacul împotriva libertăţilor civile. Există un ton anume și o atitudine care unesc jurnaliștii, activiștii și cititorii mei, oameni care sunt la fel de alarmaţi de aceste tendinţe. M-am gândit că ar fi dificil pentru cineva care nu crede cu adevărat și nu simte această îngrijorare să o reproducă atât de precis, cu atâta autenticitate.

Într-unul dintre ultimele pasaje ale e-mailurilor primite de Laura, corespondentul ei scria că face ultimii pași necesari pentru a furniza documentele. Avea nevoie de alte patru sau șase săptămâni și ar trebui să așteptăm să ne dea de veste. Ne asigura că o va face.

După trei zile, eu și Laura ne-am întâlnit din nou, de această dată în Manhattan și cu un alt e-mail de la informatorul nostru anonim, în care acesta explica de ce vrea să își riște

libertatea, să se expună pericolului de a fi închis pe termen lung, pentru a dezvălui aceste documente. Acum eram și mai convins: sursa noastră era reală, dar, așa cum i-am spus partenerului meu, David Miranda, în timpul zborului către casă, spre Brazilia, eram hotărât să îmi scot toate acestea din minte. „S-ar putea să nu se întâmple. Ar putea să se răzgândească. Ar putea fi prins.“ David este o persoană cu o intuiţie puternică și era în mod straniu sigur. „Este real. El este real. Se va întâmpla“, a afirmat el. „Și va fi ceva uriaș.“

După întoarcerea la Rio nu am mai primit nici o veste timp de trei săptămâni. Aproape că nu m-am mai gândit la sursă pentru că tot ce puteam să fac era să aștept. Apoi, pe 11 mai, am primit un e-mail de la un expert tehnic cu care eu și Laura lucraserăm în trecut. Cuvintele lui erau criptice, dar înţelesul era clar: „Salut, Glenn, revin cu informații privind învăţarea modului de funcţionare a PGP. Ai o adresă la care să îţi trimit ceva ca să te ajut să începi săptămâna viitoare?“

Sunt sigur că ce voia să trimită era ceea ce aveam nevoie pentru a începe să lucrez la documentele informatorului secret. Aceasta, în schimb, însemna că Laura avea vești de la corespondentul nostru anonim și primise ceea ce așteptam.

Tehnicianul a trimis apoi un pachet prin Federal Express, care urma să ajungă în două zile. Nu știam la ce să mă aștept: un program sau chiar documentele? În următoarele 48 de ore mi-a fost imposibil să mă concentrez la altceva. Dar în ziua la care era programată livrarea, s-a făcut ora 17.30, a trecut și nu a ajuns nimic. Am sunat la FedEx și mi s-a spus că pachetul a fost reţinut la vamă din „motive necunoscute“. Au trecut două zile. Apoi cinci. Apoi o săptămână întreagă. În fiecare zi FedEx spunea același lucru – că pachetul este reţinut de vameși din motive necunoscute.

Am cochetat pentru scurt timp cu suspiciunea că autorităţile guvernamentale – americane, braziliene sau altele – erau responsabile de această întârziere pentru că știau ceva, dar

am ajuns la explicaţia mult mai probabilă că este vorba despre o coincidenţă, fiind doar una dintre problemele birocratice.

La acel moment, Laura era foarte reticentă în a discuta despre acest lucru la telefon sau online, așa că nu știam exact ce se află în pachet.

În cele din urmă, după zece zile de când mi-a fost trimis pachetul, FedEx l-a livrat. Am desfăcut plicul și am găsit două dispozitive USB alături de o notă tipărită care conţinea instrucţiuni detaliate despre folosirea diverselor programe menite să ofere securitate maximă, precum și numeroase fraze de acces pentru criptarea conturilor de e-mail și alte programe de care nu auzisem niciodată.

Nu aveam nici o idee ce înseamnă toate acestea. Nu mai auzisem despre aceste programe specifice înainte, deși știam despre frazele de acces, practic parole lungi care conţin litere diferenţiate în funcţie de majuscule și minuscule și semne de punctuaţie înșirate la întâmplare, care au ca scop să le facă dificil de spart. Cu Poitras, foarte reticentă să vorbească la telefon sau online, încă eram frustrat: în sfârșit intrasem în posesia a ceea ce așteptam, dar fără nici un indiciu care să mă orienteze în vreo direcţie.

Aveam să descopăr în curând, de la cel mai bun ghid posibil.

În ziua în care a venit pachetul, în jur de 20 mai, Laura mi-a spus că trebuie să vorbim urgent, dar numai prin chat-ul OTR (off-the-record), un instrument criptat de discuţii sigure online. Am mai folosit OTR și înainte și m-am descurcat să instalez programul de chat, am deschis un cont și am adăugat numele de utilizator al Laurei la „lista mea de prieteni“. Ea a apărut instantaneu.

Am întrebat dacă acum am acces la documente secrete. Ele vor veni la mine doar de la sursă, mi-a spus ea, nu de la ea. Laura a adăugat apoi o informaţie nouă surprinzătoare, că trebuie să mergem la Hong Kong imediat ca să ne întâlnim cu sursa noastră. Acum eram perplex. Ce făcea în Hong Kong cineva cu acces la documente secrete ale administraţiei SUA?

Am presupus că sursa noastră anonimă era în Maryland sau în nordul statului Virginia. Ce avea de-a face Hong Kongul cu toată această poveste? Eram dispus să călătoresc oriunde, bineînţeles, dar voiam mai multe informaţii despre ce se întâmplă. Dar faptul că Laura nu putea să vorbească liber ne obliga să amânăm această discuţie.

M-a întrebat dacă vreau să călătoresc la Hong Kong în următoarele câteva zile. Voiam să fiu sigur că merită, adică: obţinuse confirmarea că sursa este reală? A răspuns criptic: „Bineînţeles, nu ţi-aș cere să mergi la Hong Kong dacă nu ar fi așa“. Am presupus că acest lucru însemna că a primit unele documente serioase din partea sursei.

Dar mi-a spus și despre o problemă nou apărută. Sursa era supărată de cum ajunseseră lucrurile atât de departe, în special despre o nouă turnură: posibila implicare a cotidianului *Washington Post*. Laura a spus că este vital să vorbesc cu el direct, să îl asigur și să îi calmez temerile tot mai mari.

Într-o oră, sursa însăși mi-a trimis un e-mail.

Acest e-mail venea de la Verax@[redacted]. *Verax* înseamnă „cel care spune adevărul“ în latină. Titlul era „Trebuie să vorbim“.

„Lucrez la un proiect major cu câţiva prieteni comuni“, începea e-mailul, sugerându-mi că este el sursa anonimă, referindu-se clar la legăturile sale cu Laura.

„Trebuie să renunţi la o călătorie pe termen scurt pentru a te întâlni cu mine. Trebuie să fii implicat în această poveste“, a scris el. „Există vreo modalitate prin care să vorbim cât mai repede? Înţeleg că nu ai făcut prea multe în ceea ce privește siguranţa infrastructurii, dar mă voi descurca cu ce ai“. A sugerat să vorbim prin OTR și mi-a dat numele lui de utilizator.

Nu eram sigur ce voia să spună cu „renunţarea la o călătorie pe termen scurt“. Mi-am exprimat nedumerirea faţă de faptul că era în Hong Kong, dar cu siguranţă nu am refuzat să merg acolo. Am pus aceasta pe seama proastei comunicări și am răspuns imediat. „Vreau să fac tot posibilul pentru a fi implicat“,

i-am spus, sugerându-i că putem vorbi imediat pe OTR. L-am adăugat pe lista mea de prieteni din OTR și am așteptat.

În 15 minute, computerul meu a scos un clinchet, semnalându-mi că a intrat. Ușor nervos, am dat click pe numele lui și am scris „salut“. A răspuns și m-am trezit vorbind direct cu cineva cu care presupuneam, la momentul respectiv, că dezvăluise mai multe documente secrete despre programele de supraveghere ale SUA și care voia să dezvăluie mai multe.

Imediat i-am spus că sunt absolut implicat în subiect. „Vreau să fac tot ce trebuie pentru a relata despre acest subiect“, i-am spus. Sursa – al cărei nume, loc de muncă, vârstă și toate celelalte atribute îmi erau necunoscute – a întrebat dacă aș veni la Hong Kong să mă întâlnesc cu el. Nu am întrebat de ce era la Hong Kong; voiam să evit să pară că aș fi căutat informaţii.

Într-adevăr, de la început am decis să îl las să preia inițiativa. Dacă voia ca eu să știu de ce era în Hong Kong, mi-ar fi spus. Și dacă voia ca eu să știu ce documente are și plănuiește să mi le ofere, mi-ar fi spus de asemenea. Această postură pasivă era dificilă pentru mine. Ca fost avocat și actual jurnalist, sunt obișnuit să chestionez agresiv atunci când vreau răspunsuri și aveam sute de lucruri pe care voiam să le aflu.

Dar am presupus că situaţia lui este delicată. Oricare ar fi fost adevărul, știam că această persoană era hotărâtă să facă ceea ce administraţia americană considera că este o infracţiune gravă. Era clar după cât de îngrijorat era de siguranţa comunicaţiilor a căror discreţie era vitală. Și m-am gândit – de vreme ce aveam atât de puţine informaţii despre cel cu care vorbesc, despre cum gândește, despre motivele și temerile lui – că această precauţie și reţinere din partea lui sunt imperative. Nu voiam să îl sperii, așa că mi-am impus să las informaţia să vină la mine mai degrabă decât să încerc să o smulg.

„Bineînţeles că voi veni la Hong Kong“, am spus, în continuare fără să am vreo idee de ce se află acolo, din toate locurile posibile, sau de ce vrea ca eu să merg acolo.

Am vorbit online în acea zi timp de două ore. Principala lui îngrijorare era ce se va întâmpla cu unele documente ale NSA despre care, cu acordul lui, Poitras vorbise cu un reporter al *Washington Post*, Barton Gellman. Documentele se refereau la un subiect specific despre un program numit PRISM, care permitea NSA să colecteze informaţii private de la cele mai mari companii de internet, inclusiv Facebook, Google, Yahoo! și Skype.

Mai degrabă decât să relateze subiectul rapid și agresiv, *Washington Post* reunise o echipă mare de avocaţi care au făcut tot felul de cereri și au emis tot felul de avertizări catastrofale. Potrivit sursei, aceasta arăta că *Post*, gestionând ceea ce credea a fi o oportunitate jurnalistică fără precedent, era mânat de frică mai degrabă decât de convingere și hotărâre. El era, de asemenea, furios pentru că *Post* implicase atât de multe persoane, fiindu-i teamă că aceste discuţii i-ar putea pune în pericol siguranța.

„Nu îmi place cum evoluează lucrurile“, mi-a spus. „Voiam ca altcineva să relateze această primă poveste despre PRISM astfel încât tu să te poţi concentra pe arhiva mai vastă, în special pe spionajul de masă intern, dar acum chiar vreau ca tu să fii cel care relatează despre acest lucru. Îți citesc de multă vreme articolele“, a spus el, „și știu că vei fi agresiv și nu îţi va fi teamă în ceea ce vei face“.

„Sunt pregătit și nerăbdător“, i-am spus. „Hai să stabilim acum ce trebuie să fac.“

„Mai înainte de toate trebuie să vii la Hong Kong“, a spus el. Se întorcea mereu la aceasta: *vino la Hong Kong imediat*.

Celălalt subiect important pe care l-am discutat în acea primă conversaţie a fost scopul lui. Știam din e-mailurile pe care Laura a trebuit să mi le arate că se simţea obligat să spună lumii despre aparatul de spionaj masiv pe care administraţia americană îl construise în secret. Dar ce spera să obţină?

„Vreau să generez o dezbatere la nivel mondial despre dreptul la intimitate, despre libertatea internetului și pericolele

supravegherii din partea statului", a spus el. „Nu îmi este teamă de ce se va întâmpla cu mine. Am acceptat faptul că viața mea se va sfârși probabil pentru că fac acest lucru. Sunt împăcat cu aceasta. Știu că tot ce fac este corect."

Apoi a spus ceva surprinzător: „Vreau să mă identific cu persoana din spatele acestei dezvăluri. Cred că am o obligație de a explica de ce fac acest lucru și ce sper să obțin". Mi-a spus că a scris un document pe care voia să îl posteze pe internet când se deconspira ca sursă, un manifest prointimitate, antisupraveghere, pentru ca oamenii din lumea întreagă să îl semneze, arătând că există un sprijin global pentru protejarea intimității.

În pofida consecințelor aproape sigure ale deconspirării lui – o lungă perioadă de închisoare, dacă nu mai rău –, el era, și o spunea mereu, „împăcat" cu aceste consecințe. „Am o singură teamă atunci când fac toate aceste lucruri", a declarat el, și anume aceea „că oamenii vor vedea aceste documente și vor ridica din umeri, că vor spune «am bănuit că acest lucru se întâmplă și nu ne pasă». Singurul lucru de care sunt îngrijorat este că voi face toate acestea pentru nimic".

„Mă îndoiesc serios că acest lucru se va întâmpla", l-am asigurat, dar nu eram convins că într-adevăr așa cred. Știam din anii în care scrisesem despre abuzurile NSA că poate fi dificil să generezi îngrijorări grave în legătură cu supravegherea secretă din partea statului: invadarea intimității și abuzul de putere pot fi văzute drept chestiuni abstracte, care cu greu îi fac pe oameni să le pese visceral. Mai mult, problema supravegherii este invariabil complexă, ceea ce face și mai greu de implicat publicul la scară largă.

Dar am simțit că de data aceasta era diferit. Mass-media acordă atenție atunci când există scurgeri de documente secrete. Iar faptul că avertizarea venea din partea cuiva din interiorul aparatului de securitate națională – mai degrabă decât din partea unui avocat al Uniunii Americane pentru Libertăți

Civile sau a unui avocat pentru libertăţi civile – cu siguranţă că ar fi adăugat un plus de greutate.

În acea noapte am vorbit cu David despre călătoria la Hong Kong. Încă eram reticent în a-mi lăsa toată munca pentru a zbura în cealaltă parte a lumii și a mă întâlni cu cineva despre care nu știam nimic, nici măcar numele, mai ales că nu aveam nici o dovadă reală că este cine spune că este. Ar fi putut fi o totală pierdere de timp – sau o capcană ori vreun complot ciudat.

„Ar trebui să-i spui că vrei să vezi câteva documente mai întâi, ca să îţi dai seama că este serios și că merită, din punctul tău de vedere“, a sugerat David.

Ca de obicei, i-am acceptat sfatul. Când am intrat pe OTR în dimineaţa următoare, am spus că plănuiesc să plec către Hong Kong în câteva zile, dar mai întâi vreau să văd unele documente ca să înţeleg ce fel de dezvăluiri este pregătit să facă.

Pentru aceasta, mi-a spus din nou să instalez diverse programe. Atunci am petrecut câteva zile online în timp ce sursa mă ghida, pas cu pas, în instalarea și folosirea fiecărui program, inclusiv, în cele din urmă, a programului de criptare PGP. Știind că sunt începător, a dat dovadă de multă răbdare, efectiv la nivelul „Apasă pe butonul albastru, acum apasă OK, acum mergi la următorul ecran“.

Îmi tot ceream scuze pentru lipsa mea de competenţă, pentru că îi consum ore întregi din timpul lui pentru a mă învăţa aspectele elementare ale unei comunicaţii securizate. „Nu-ţi face griji“, a spus el, „multe dintre ele nu prea au sens. În plus, am mult timp liber în momentul ăsta.“

Odată programele instalate, am primit un fișier care conţinea aproximativ 25 de documente: „Doar o mostră: vârful vârfului aisbergului“, a explicat el în mod tentant.

Am dezarhivat fișierul, am văzut lista de documente și am deschis la întâmplare unul dintre ele. În partea de sus a paginii, scris cu roșu, apărea un cod: „TOP SECRET//COMINT/NOFORN/“.

Aceasta însemna că documentul fusese catalogat legal ca fiind strict secret, destinat comunicării în cadrul serviciilor de informaţii (COMINT) și interzis distribuirii cetăţenilor străini, organizaţiilor internaţionale sau partenerilor de coaliţie (NOFORN). Era de o claritate incontestabilă: o comunicare foarte confidenţială din partea NSA, una dintre cele mai secretoase agenţii a celui mai puternic guvern din lume. Nici un document atât de semnificativ nu se mai scursese de la NSA, nimic în istoria de șase decenii a agenţiei. Acum eram în posesia a aproximativ 25 de astfel de documente. Iar persoana cu care petrecusem mai multe ore discutând în ultimele două zile avea multe, mult mai multe să îmi dea.

Acest prim document era un manual pentru oficialii NSA despre cum să instruiască analiștii în privinţa noilor capacităţi de supraveghere. Se discuta în termeni cuprinzători despre tipul de informaţie pe care analiștii ar putea-o căuta (adrese de e-mail, date de localizare IP – Internet Protocol, numere de telefon) și tipul de date pe care le puteau primi ca răspuns (conţinutul unor e-mailuri, „metadate“ telefonice, arhive ale discuţiilor online). Practic, spionam oficialii NSA în timp ce își instruiau analiștii în legătură cu modul în care să își supravegheze ţintele.

Inima îmi bătea cu putere. A trebuit să mă opresc din citit și să mă plimb prin casă de câteva ori pentru a înţelege ceea ce tocmai văzusem și pentru a mă calma suficient încât să mă pot concentra pe lectura fișierelor. M-am întors la laptopul meu și am deschis la întâmplare un alt document, o prezentare strict secretă în PowerPoint, intitulată „PRISM/US-984XN REZUMAT“. Fiecare pagină purta logourile a nouă dintre cele mai mari companii de internet, inclusiv Google, Facebook, Skype și Yahoo!.

Primul slide expunea un program prin care NSA intrase în posesia a ceea ce numea „o colecţie direct de pe serverele acestor furnizori de servicii americani: Microsoft, Yahoo, Google, Facebook, Paltalk, AOL, Skype, YouTube, Apple“. Un

grafic prezenta datele la care fiecare dintre aceste companii se alăturase programului.

Am devenit din nou agitat, a trebuit să mă opresc din citit.

Sursa mi-a spus, de asemenea, că îmi trimite un document de mari dimensiuni pe care nu îl voi putea accesa până când nu va veni momentul potrivit. Am decis să las deoparte această afirmaţie codificată, dar semnificativă pentru moment, consecvent cu hotărârea mea de a-l lăsa pe el să decidă când primesc informaţia, dar și pentru că eram tulburat de ce aveam în faţa mea.

De la prima privire asupra acestor câtorva documente am știut două lucruri: că trebuia să ajung la Hong Kong imediat și că voi avea nevoie de sprijin instituţional substanţial pentru a relata acest lucru. Aceasta însemna să implic *Guardian*, ziarul și site-ul de știri cu care colaboram ca editorialist zilnic de nouă luni. Acum eram pe cale să îi implic în ceea ce știam deja că va fi un subiect exploziv major.

Folosind Skype, am contactat-o pe Janine Gibson, care era redactorul-șef britanic al ediţiei americane a *Guardian*. Acordul meu cu *Guardian* era să am independenţă editorială totală, ceea ce însemna că nimeni nu îmi putea edita sau corecta articolele înainte de publicare. Mi-am scris articolele și le-am publicat eu însumi direct pe internet. Singura excepţie la această înţelegere era să îi avertizez dacă ceea ce scriam putea avea consecinţe juridice pentru ziar sau prezenta o dilemă jurnalistică neobișnuită. Acest lucru se întâmplase de foarte puţine ori în cele nouă luni, doar o dată sau de două ori, ceea ce însemna că avusesem o interacţiune foarte redusă cu editorii *Guardian*.

Evident, dacă vreun subiect justifica o avertizare, atunci acesta era. De asemenea, știam că voi avea nevoie de resursele și sprijinul ziarului.

„Janine, am un subiect monumental“, am spus fără vreo introducere. „Am o sursă care are acces la ceea ce pare a fi un volum mare de documente strict secrete de la NSA. Mi-a dat

deja câteva și sunt șocante. Dar spune că are mai multe, mult mai multe. Din anumite motive, este în Hong Kong. Încă nu am nici o idee de ce, și vrea să mă duc acolo să mă întâlnesc cu el și să primesc restul. Ceea ce mi-a dat și pe ce am reușit să mă uit mi se pare destul de șocant..."

Gibson m-a întrerupt: „Cum mă suni?"

„De pe Skype."

„Nu cred că ar trebui să vorbim despre asta la telefon și sigur nu pe Skype", a spus ea cu înţelepciune și mi-a propus să iau un avion către New York imediat, astfel încât să discutăm faţă în faţă.

Planul meu, despre care i-am spus Laurei, era să zbor la New York, să arăt documentele celor de la *Guardian*, să le stârnesc interesul despre subiect și apoi să îi determin să mă trimită la Hong Kong să mă văd cu sursa. Laura a fost de acord să ne întâlnim la New York, apoi intenţionam să călătorim împreună către Hong Kong.

A doua zi plecam de la Rio către JFK cu un zbor de noapte și pe la ora 9.00 dimineaţa, în ziua următoare, vineri 31 mai, m-am cazat la hotelul meu din Manhattan și apoi m-am întâlnit cu Laura. Primul lucru pe care l-am făcut a fost să mergem la un magazin să cumpărăm un laptop care să îmi servească drept „dispozitiv de protecţie", un computer care nu fusese niciodată conectat la internet. Este mult mai dificil să supraveghezi un computer care nu are internet. Pentru a monitoriza un computer neconectat, un serviciu de informaţii ca NSA ar trebui să folosească metode mult mai complicate, precum obţinerea accesului fizic la computer și amplasarea unui dispozitiv de supraveghere pe hard disk. Ținerea computerului închis tot timpul ajută la preîntâmpinarea unei astfel de invadări a intimității. Aveam să folosesc acest laptop nou pentru a lucra cu materialele pe care nu le voiam monitorizate, precum documentele secrete ale NSA, fără teama de a fi detectate.

Am băgat noul computer în rucsac și am mers pe jos cu Laura până la biroul din Soho al *Guardian*.

Gibson ne aștepta când am ajuns. Am mers direct în biroul ei, unde ni s-au alăturat Stuart Millar, adjunctul lui Gibson. Laura a rămas afară. Gibson nu o cunoștea pe Laura și voiam să discutăm liber. Nu știam cum vor reacţiona editorii *Guardian* la ceea ce aveam. Nu mai lucrasem cu ei până atunci, cu siguranţă nu pe un subiect care să se apropie măcar de acest nivel de gravitate și importanţă.

După ce am încărcat fișierele primite de la sursă pe laptop, Gibson și Millar s-au așezat împreună la o masă și au citit documentele, scoţând periodic câte un „uau“ și exclamaţii similare. M-am așezat pe o canapea și i-am privit în timp ce citeau, observând șocul care li se întipărea pe feţe atunci când începeau să conștientizeze importanța a ceea ce deţineam. De fiecare dată când terminau un document, săream să li-l arăt pe următorul. Uimirea lor nu făcea decât să se intensifice.

În plus faţă de cele 24 de documente ale NSA pe care le trimisese, sursa inclusese și o declarație pe care intenţiona să o publice, în care cerea semnături de solidaritate în favoarea vieţii private și împotriva supravegherii. Declarația era dramatică și dură, dar era de așteptat, având în vedere alegerile dramatice și dure pe care trebuise să le facă, alegeri care aveau să-i schimbe viaţa pentru totdeauna. Înţelegeam motivul pentru care cineva care fusese martor la construcţia din umbră a unui sistem universal de supraveghere din partea statului, fără nici o supervizare sau verificare, ar fi grav alarmat de ce a văzut și de pericolele presupuse de acest lucru. Bineînţeles că tonul lui era extrem; fusese atât de alarmat, încât luase o decizie extraordinară de a face ceva curajos și de anvergură. Am înţeles motivul acestui ton, deși eram îngrijorat de reacţia lui Gibson și Millar la citirea declarației. Nu voiam să creadă că avem de-a face cu cineva instabil emoţional, mai ales că, având în vedere că petrecusem multe ore vorbind cu el, știam că este foarte raţional și implicat.

Frica mea s-a adeverit imediat. „Unora le va suna nebunesc“, a rostit Gibson.

„Unele persoane și mass-media pro-NSA vor spune că este ceva similar lui Ted Kaczynski“*, sunt de acord. „Dar în cele din urmă documentele sunt cele care contează, nu el sau motivele sale de a ni le oferi. Și, în afară de aceasta, oricine face ceva atât de extrem va avea gânduri extreme. Este inevitabil.“

Pe lângă declarație, Snowden redactase o scrisoare către jurnaliștii cărora le-a dat arhiva sa de documente. Aceasta intenţiona să explice scopul și obiectivele sale și anticipa cum va fi demonizat:

> Singurul meu motiv este să informez publicul cu privire la ce s-a făcut în numele său şi ce s-a făcut împotriva sa. Administrația americană, în conspirație cu statele subordonate, dintre care cele mai importante sunt așa-numitele Five Eyes [Cinci Ochi] – Marea Britanie, Canada, Australia şi Noua Zeelandă –, a generat un sistem de supraveghere secretă universală față de care nu există scăpare. Ei îşi protejează sistemele interne de supravegehere a cetățenilor prin secrete şi minciuni şi se protejează ele însele de ultraj în eventualitatea unor scurgeri de informații supraaccentuând protecțiile limitate pe care au ales să le acorde celor guvernați...
>
> Documentele anexate sunt reale şi originale şi sunt furnizate pentru a oferi o înțelegere a modului în care funcționează sistemul de supraveghere global şi pasiv, astfel încât să se poată dezvolta protecții împotriva acestuia. În ziua în care am scris aceste cuvinte, toate înregistrările noi ale comunicațiilor care pot fi absorbite şi catalogate de acest sistem urmează să fie deținute timp de [] ani, iar noi „Depozite Masive de Date“ (sau eufemistic Depozite de Date din „Misiune“) sunt construite şi desfăşurate în lumea întreagă, cel mai mare fiind noul centru de date din Utah. În timp ce eu mă rog ca publicul să conştientizeze şi să genereze o dezbatere care să ducă la reformă, am în vedere că politicile omenirii se schimbă în timp şi chiar Constituția

* Matematician american, cunoscut și sub numele de Unabomber, care a condus o campanie de atentate cu bombă prin poștă, între 1978–1995, pentru a protesta împotriva societății tehnico-industriale (n.red.)

> este subminată atunci când apetitul pentru putere o cere. În cuvinte istorice: Să nu mai vorbim despre credința în om, ci să-l încătuşăm pe acesta pentru nereguli cu lanțurile criptografiei.

Am recunoscut instantaneu ultima frază ca o interpretare a unui citat din Thomas Jefferson, din 1798, pe care îl amintesc frecvent în scrierile mele: „Când se pune problema puterii, prin urmare, să nu mai auzim de încrederea în om, ci să-l încătușăm pe acesta pentru nereguli cu lanţurile Constituţiei".

După ce au văzut toate documentele, inclusiv scrisoarea lui Snowden, Gibson și Millar au fost convinși. „Practic", a conchis Gibson în două ore de la sosirea mea în acea dimineaţă, „trebuie să mergi la Hong Kong cât mai repede posibil, cum ar fi mâine, corect?"

Guardian era cooptat în echipă. Misiunea mea în New York fusese îndeplinită. Acum știam că Gibson se angajase să urmărească subiectul agresiv, cel puţin pentru moment. În acea după-amiază, eu și Laura am vorbit cu persoana care se ocupa de deplasări la *Guardian* pentru a ajunge la Hong Kong cât mai repede posibil. Cea mai bună opţiune era un zbor fără escală de 16 ore cu Cathay Pacific care pleca de pe JFK în dimineaţa zilei următoare. Dar tocmai când începeam să sărbătorim iminenta noastră întâlnire cu sursa, s-a ivit o complicaţie.

La sfârșitul zilei, Gibson a declarat că vrea să implice un reporter vechi al *Guardian*, Ewen MacAskill, care lucra la ziar de 20 de ani. „Este un jurnalist extraordinar", a spus ea. Având în vedere amploarea lucrului la care mă angajam, știam că voi avea nevoie de alţi reporteri ai *Guardian* pentru acest subiect și nu am avut nici o obiecţie în principiu. „Aș vrea ca Ewen să meargă cu tine la Hong Kong", a adăugat ea.

Nu îl cunoșteam pe MacAskill. Mai mult, nici sursa nu îl cunoștea și, din câte știa, doar Laura și cu mine veneam la Hong Kong. Iar Laura, care plănuise totul cu meticulozitate, avea să fie furioasă la această schimbare bruscă de planuri.

Am avut dreptate. „În nici un caz. Categoric nu“, a răspuns ea. „Nu putem adăuga pur și simplu o persoană nouă în ultimul minut. Și nu îl cunosc deloc. Cine l-a verificat?“

Am încercat să îi explic care credeam că este motivul lui Gibson. Nu știam și nu aveam încredere încă în *Guardian*, nu când era vorba despre un subiect uriaș ca acesta, și am presupus că și ei simţeau același lucru în privinţa mea. Având în vedere cât risca *Guardian*, m-am gândit că voiau ca o persoană pe care o cunoșteau foarte bine – cineva care era de multă vreme în companie – să le spună ce se întâmplă cu sursa și să îi asigure că acest subiect era unul pe care ei trebuiau să îl abordeze. În afară de aceasta, Gibson avea nevoie de sprijinul total și aprobarea editorilor *Guardian* din Londra, care mă cunoșteau și mai puţin decât ea. Voia probabil să aducă pe cineva care putea să facă Londra să se simtă în siguranţă, iar Ewen se potrivea perfect cu acest plan.

„Nu-mi pasă“, a spus Laura. „Să călătorim cu o a treia persoană, un străin, ar putea să atragă supravegherea noastră sau să sperie sursa“. Ca un compromis, Laura a sugerat ca ei să îl trimită pe Ewen după câteva zile, după ce noi stabileam contactul cu sursa în Hong Kong și îi câștigam încrederea. „Ai toate pârghiile. Spune-le că nu îl pot trimite pe Ewen până nu suntem gata“.

M-am întors la Gibson cu ceea ce părea un compromis deștept, dar ea era hotărâtă. „Ewen o să zboare cu tine la Hong Kong, dar nu se va întâlni cu sursa până când tu și Laura nu veţi spune că sunteţi gata.“

În mod clar, pentru *Guardian* era crucial ca Ewen să vină cu noi la Hong Kong. Gibson avea nevoie de asigurări în legătură cu ce se întâmpla acolo și pentru a calma orice îngrijorări pe care le-ar fi putut avea șefii ei din Londra. Dar Laura era la fel de neclintită că ar trebui să călătorim singuri. „Dacă sursa ne supraveghează la aeroport și vede această a treia persoană neașteptată pe care nu o cunoaște, se va speria și va renunța să ne contacteze. În nici un caz.“ Ca un diplomat din cadrul

Departamentului de Stat care face drumuri între adversarii din Orientul Mijlociu în speranţa futilă de a negocia o înţelegere, m-am întors la Gibson, care a dat un răspuns vag cum că Ewen va veni după câteva zile. Sau poate asta am vrut eu să aud.

Pe de altă parte, târziu în seara respectivă am aflat de la persoana care se ocupa de deplasări că biletul lui Ewen fusese cumpărat – pentru ziua următoare, la bordul aceluiași avion. Iar ei îl trimiteau cu acel avion indiferent de situaţie.

În mașină, pe drumul către aeroport, eu și Laura am avut prima și singura ceartă. Am anunţat-o imediat ce ieșeam cu mașina din hotel și a explodat de furie. Puneam în pericol întregul aranjament, a insistat ea. Era o inconștienţă să aducem pe cineva străin în acest stadiu. Nu avea încredere în cineva care nu fusese verificat și m-a acuzat că las *Guardian* să ne pună planul în pericol.

Nu puteam să îi spun Laurei că îngrijorările ei erau lipsite de fundament, dar am încercat să o conving că *Guardian* fusese insistent, că nu avusesem de ales. Iar Ewen se va întâlni cu sursa doar atunci când noi vom fi pregătiţi.

Laurei nu îi păsa. Ca să o calmez, m-am oferit chiar să nu merg, o sugestie pe care a respins-o imediat. Am păstrat o tăcere jalnică, furioasă, timp de zece minute, în timp ce mașina era blocată în trafic în drum spre JFK.

Știam că Laura are dreptate: nu ar fi trebuit să se întâmple așa și am rupt tăcerea spunându-i acest lucru. Apoi i-am propus să îl ignorăm pe Ewen și să îl excludem, să pretindem că nu este cu noi. „Suntem de aceeași parte“, am ispitit-o pe Laura. „Hai să nu ne certăm. Având în vedere ce este în joc, aceasta nu va fi prima dată când lucrurile o să ne scape de sub control.“ Am încercat să o conving pe Laura că ar trebui să rămânem concentraţi pe munca împreună pentru a depăși obstacolele. În scurt timp am revenit la o stare de calm.

După ce am ajuns în apropierea aeroportului JFK, Laura a scos un stick de memorie din rucsac. „Ghicești ce este?“, a întrebat ea cu o privire foarte serioasă.

„Ce?“

„Documentele“, a spus ea. „Toate.“

Ewen era deja la poarta de îmbarcare când am ajuns noi. Laura și cu mine eram politicoși, dar reci, asigurându-ne că se simte exclus, că nu are nici un rol până când nu eram noi pregătiţi să îi acordăm unul. El era singura ţintă prezentă a iritării noastre, așa că îl tratam ca pe un bagaj în plus care ni se pusese în cârcă. Era nedrept, dar eram prea distras de perspectiva comorilor de pe stickul de memorie al Laurei și de semnificaţia a ceea ce făceam, pentru a ne mai păsa de Ewen.

Laura mi-a făcut un instructaj de cinci minute despre sistemul de securizare a computerului în mașină și mi-a spus că intenţionează să doarmă în avion. Mi-a dat stickul USB și mi-a sugerat să încep să mă uit peste setul ei de documente. Odată ajunși la Hong Kong, mi-a spus ea, sursa se va asigura că voi avea acces deplin la propriul meu set complet.

După ce avionul a decolat, am scos noul meu computer protejat, am inserat stickul USB al Laurei și am urmat instrucţiunile ei pentru încărcarea fișierelor.

În următoarele 16 ore, în pofida extenuării mele, nu am făcut nimic altceva decât să citesc document după document, luând notiţe febril. Multe fișiere erau la fel de impresionante și șocante cum era acea prezentare iniţială în PowerPoint a PRISM pe care o văzusem în Rio. Multe dintre ele erau și mai și.

Unul dintre primele pe care le-am citit era un ordin din partea tribunalului secret pentru Legea privind supravegherea activităţilor străine de spionaj (FISA), care a fost creat de Congres în 1978, după ce Comisia Church a descoperit interceptări abuzive ale administraţiei care durau de zeci de ani. Ideea din spatele formării sale a fost ca guvernul să obţină permisiunea tribunalului FISA înainte de a putea continua supravegherea electronică, pentru prevenirea unor abuzuri similare. Nu văzusem niciodată până atunci un ordin al tribunalului FISA. Aproape nimeni nu văzuse. Tribunalul este una dintre cele

mai secrete instituţii ale administraţiei. Toate hotărârile sale sunt marcate automat strict secret și doar un grup restrâns de persoane are acces la deciziile sale.

Hotărârea pe care am citit-o în avionul către Hong Kong era uimitoare din mai multe motive. Aceasta ordona Verizon Business să predea NSA „toate datele apelurilor telefonice“ pentru „comunicaţiile (i) între Statele Unite și străinătate; și (ii) toate din Statele Unite, inclusiv apelurile telefonice locale“. Aceasta însemna că NSA colecta în secret și fără discriminare date telefonice de la zeci de milioane de americani, cel puţin. Practic, nimeni nu știa că administraţia Obama face așa ceva. Acum, cu această hotărâre, nu numai că știam despre acest lucru, dar aveam ca dovadă și ordinul tribunalului secret.

Mai mult decât atât, ordinul tribunalului specifica faptul că strângerea în masă a datelor telefonice americane era autorizată de Secţiunea 215 din Patriot Act*. Aproape mai mult decât hotărârea în sine, această interpretare radicală a Patriot Act era deosebit de șocantă.

Ce a făcut Patriot Act atât de controversat atunci când a fost adoptat după atacurile din 11 septembrie a fost că Secţiunea 215 cobora standardul pe care trebuia să îl întrunească administraţia pentru a obţine „documente de afaceri“, de la „cauză probabilă“ la „relevanţă“. Aceasta însemna că, pentru a obţine documente extrem de sensibile și invazive – precum istoric medical, tranzacţii bancare sau date telefonice –, Biroul Federal de Investigaţii trebuia să demonstreze doar că acele documente sunt „relevante“ pentru o investigaţie în așteptare.

Dar nimeni – nici chiar membrii republicani agresivi ai Camerei Reprezentanţilor care au elaborat Patriot Act în 2001 sau cei mai devotaţi susţinători ai libertăţilor civile care au

* Lege adoptată în octombrie 2001 de Congresul SUA ca urmare a atacurilor de la 11 septembrie. Gândit ca un set de măsuri temporare împotriva terorismului, Patriotic Act este contestat în SUA deoarece multe dintre măsurile stipulate limitează dreptul la viață privată al cetățenilor. (n.red.)

descris legea în cea mai amenințătoare lumină – nu s-a gândit că legea acorda administrației americane prerogativele de a colecta date despre fiecare, în masă și fără discriminare. Era exact ceea ce conchidea acest ordin secret al tribunalului FISA, deschis pe laptopul meu în timp ce zburam către Hong Kong, atunci când cerea de la Verizon să predea NSA toate datele telefonice pentru toţi clienţii săi americani.

Timp de doi ani, senatorii democraţi Ron Wyden din Oregon și Mark Udall din New Mexico au mers prin ţară avertizând că americanii ar putea fi „uimiţi să afle“ despre „interpretările secrete ale legii“ pe care administraţia Obama o folosea pentru a se învesti cu puteri de spionare vaste și necunoscute. Dar deoarece aceste activităţi de spionaj erau secretizate, cei doi senatori, care erau membri ai Comisiei pentru Serviciile de Informaţii din Senat, au renunțat să divulge publicului ce au descoperit atât de amenințător, în pofida scutului legal de imunitate acordat membrilor Congresului de Constituţie pentru a face astfel de dezvăluiri dacă aleg acest lucru.

Am știut imediat ce am văzut ordinul tribunalului FISA că aceasta era cel puţin o parte din programele de supraveghere abuzive și radicale în privinţa cărora Wyden și Udall încercaseră să avertizeze ţara. Am recunoscut instantaneu semnificaţia ordinului. Abia așteptam să îl public, fiind sigur că darea sa în vileag va atrage după sine un cutremur și că vor urma cu siguranţă apeluri la transparenţă și responsabilitate. Iar acesta era doar unul dintre sutele de documente strict secrete pe care le-am citit în drum spre Hong Kong.

Încă o dată, am simţit cum mi se schimbă perspectiva despre semnificaţia acţiunilor sursei. Acest lucru se întâmplase deja de trei ori înainte: când am văzut prima dată e-mailurile primite de Laura, apoi când am început să vorbesc cu sursa și ulterior când am citit cele aproximativ 24 de documente pe care le trimisese prin e-mail. Doar acum am simţit că încep cu adevărat să procesez adevărata amploare a scurgerii de informaţii.

În câteva ocazii în timpul zborului, Laura a venit pe rândul pe care stăteam, care se afla în faţa peretelui despărţitor al avionului. Imediat ce am văzut-o, m-am ridicat de pe scaun și am stat amândoi în spaţiul deschis din faţa peretelui despărţitor, fără cuvinte, copleșiţi și năuciţi de ceea ce aveam.

Laura lucra de ani întregi la subiectul supravegherii NSA, ea însăși fiind supusă în mod repetat abuzurilor acesteia. Am scris despre ameninţarea ridicată de supravegherea internă nesupusă constrângerilor încă din 2006, când am publicat prima mea carte, avertizând asupra radicalismului și ilegalităţii NSA. Cu această carte, amândoi am luptat cu marele zid care înconjoară secretul spionajului guvernamental: cum documentezi acţiunile unei agenţii atât de ascunse în niveluri multiple de secret oficial? În acest moment, spărsesem zidul. Aveam în posesia noastră documente care dovedeau indiscutabil tot ceea ce făcuse administraţia pentru a distruge viaţa privată a americanilor și a oamenilor din lumea întreagă.

Pe măsură ce citeam, m-au izbit două lucruri în legătură cu arhiva. Primul a fost faptul că era extraordinar de bine organizată. Sursa crease nenumărate foldere și apoi subfoldere și sub-subfoldere. Fiecare document fusese plasat exact acolo unde îi era locul. Nu am găsit nici un document clasificat greșit.

Am petrecut ani întregi apărând ceea ce consideram a fi actele eroice ale lui Chelsea (pe atunci Bradley) Manning, soldat și avertizor de integritate care a fost oripilat de comportamentul administraţiei americane – crimele sale de război și alte înșelăciuni sistematice –, încât și-a riscat libertatea pentru a dezvălui lumii întregi documente secretizate prin intermediul WikiLeaks. Dar Manning a fost criticat (pe nedrept și în mod inadecvat, cred eu) pentru presupusa scurgere de documente pe care nu le-a examinat înainte – spre deosebire de Daniel Ellsberg, au speculat criticii. Acest argument, deși lipsit de fundament (Ellsberg a fost unul dintre cei mai devotaţi apărători ai lui Manning și a părut clar că Manning cel puţin

a trecut în revistă documentele), a fost folosit frecvent pentru a submina ideea că acţiunile lui Manning au fost eroice.

Era clar că nimic de acest fel nu se putea spune despre sursa noastră din cadrul NSA. Fără îndoială că examinase cu atenţie fiecare document pe care ni-l dăduse, că înţelesese semnificaţia lor, apoi le plasase meticulos pe fiecare într-o structură organizată elegant.

Celălalt aspect care m-a frapat la arhivă a fost amploarea minciunii guvernamentale pe care o dezvăluia, dovadă pe care sursa o semnalizase corespunzător. Își denumise unul dintre primele dosare „INFORMATOR FĂRĂ LIMITE (NSA a minţit Congresul)". Acest folder conţinea zeci de documente care arătau statistici elaborate deţinute de NSA despre câte apeluri telefonice și e-mailuri interceptează agenţia. Conţinea, de asemenea, dovada că NSA colecta date telefonice și electronice despre milioane de americani în fiecare zi. BOUNDLESS INFORMANT [INFORMATOR FĂRĂ LIMITE] era numele programului NSA desemnat să cuantifice activităţile de supraveghere zilnice ale agenţiei cu o exactitate matematică. O hartă din fișier arăta că, pe o perioadă de 30 de zile care se termina în februarie 2013, o unitate a NSA colectase peste *trei miliarde* de fragmente de date de comunicare doar din sistemele de comunicaţii americane.

Sursa ne oferise dovada clară că oficialii NSA minţiseră Congresul, direct și în mod repetat, în legătură cu activităţile agenţiei. Timp de ani întregi, diverși senatori au cerut NSA o evaluare aproximativă a numărului de americani care au telefoanele și e-mailurile interceptate. Oficialii au insistat că nu pot răspunde pentru că nu au și nu pot deţine astfel de date: tocmai datele reflectate pe larg în documentele BOUNDLESS INFORMANT.

Chiar și mai semnificativ, fișierele – alături de documentele Verizon – dovedeau că oficialul de rang înalt al administraţiei Obama din domeniul securităţii naţionale, directorul Serviciilor Naţionale de Informaţii, James Clapper, a minţit

Congresul când, la 12 martie 2013, a fost întrebat de senatorul Ron Wyden: „Colectează NSA vreun fel de date despre milioane sau sute de milioane de americani?"

Răspunsul lui Clapper a fost pe cât de succint pe atât de neadevărat: „Nu, domnule".

În 16 ore de lectură aproape neîntreruptă, am reușit să parcurg doar o mică parte din arhivă. Dar în timp ce avionul ateriza în Hong Kong, știam cu siguranţă două lucruri. Primul, că sursa este o persoană foarte sofisticată și care se pricepe la politică, lucru evident din faptul că recunoscuse semnificaţia majorităţii documentelor. În plus, că este și o persoană foarte raţională. Modul în care alesese, analizase și descrisese mii de documente pe care le aveam acum în posesie dovedea acest lucru. În al doilea rând, avea să fie foarte dificil să îi negi statutul de avertizor de integritate clasic. Dacă dezvăluirea faptului că oficiali de rang înalt din domeniul securităţii interne au minţit făţiș Congresul despre programele de spionaj intern nu face din cineva în mod indiscutabil un avertizor de integritate, atunci ce anume îl face astfel?

Am știut că, cu cât va fi mai greu pentru administraţie și aliaţii săi să demonizeze sursa, cu atât mai puternic va fi efectul dezvăluirilor acesteia. Cele două direcții favorite pentru discreditarea unui avertizor de integritate – „este instabil" și „este naiv" – nu aveau să funcţioneze în acest caz.

Cu puţin timp înainte de aterizare, am citit un ultim fișier. Deși se numea „CITEȘTE-MĂ PRIMUL", l-am văzut pentru prima dată doar la sfârșitul zborului. Acest document era o altă explicaţie din partea sursei de ce m-a ales pe mine și ce aștepta să se întâmple ca urmare a acestui fapt, iar tonul și conţinutul erau similare cu cele din declarația pe care o arătasem editorilor *Guardian*.

Dar acest document cuprindea fapte pe care celălalt nu le conţinea. Includea numele sursei – a fost prima dată când l-am aflat –, alături de anticipări clare în legătură cu ce i se va întâmpla odată deconspirat. Referindu-se la evenimentele care

au precedat scandalul NSA din 2005, nota se încheia în felul următor:

> Mulți mă vor denigra pentru că am eşuat în a mă implica în relativismul național, că mi-am întors privirea de la problemele societății [mele] către rele îndepărtate, externe, pentru care noi nu avem nici autoritate, nici responsabilitate, dar cetățenia presupune datoria de a supraveghea propriul guvern înainte de a căuta să le corectezi pe altele. Aici, acum, acasă, noi îndurăm o administrație care abia permite un control limitat şi refuză responsabilitatea atunci când sunt comise infracțiuni. Când tineri marginalizați comit infracțiuni minore, noi ca societate închidem ochii atunci când suferă consecințe de neîndurat în cel mai mare sistem penitenciar din lume, dar când cei mai bogați şi mai puternici furnizori de telecomunicații din țară comit conştient zeci de mii de înşelătorii, Congresul trece peste principala lege a națiunii noastre oferind prietenilor de elită imunitate totală retroactivă – civilă şi penală – pentru infracțiuni care ar fi meritat cele mai lungi sentințe din [ ] istorie.
>
> Aceste companii... au cei mai buni avocați din țară în echipa lor şi nu suferă nici cele mai mici consecințe. Când oficiali de la cele mai înalte niveluri ale puterii, pentru a-l aminti aici în mod specific pe vicepreşedinte, sunt anchetați deoarece au condus personal o astfel de acțiune penală, ce ar trebui să se întâmple? În cazul în care credeți că ancheta ar trebui oprită, rezultatele ei secretizate într-un compartiment special pentru „Informații Controlate în mod Excepțional" numit STLW [VÂNTSTELAR], orice anchetă ulterioară exclusă pe principiul că tragerea la răspundere a celor care abuzează de putere este împotriva interesului național, că trebuie să „privim înainte, nu înapoi" şi că mai degrabă decât să se închidă programul ilegal îl veți extinde cu şi mai multe autorități, veți fi bineveniți pe coridoarele puterii nelimitate, pentru că aceasta a ajuns să fie, iar eu public documente care o dovedesc.
>
> Înțeleg că voi suferi pentru acțiunile mele şi că divulgarea acestor informații îmi marchează sfârşitul. Voi fi mulțumit dacă federația legii secrete, exonerarea inegală şi puterile executive

omnipotente care conduc lumea pe care o iubesc sunt dezvăluite chiar şi numai pentru o clipă. Dacă vrei să ajuţi, alătură-te comunităţii sursă deschisă şi luptă pentru a menţine spiritul presei viu şi internetul liber. Am văzut cele mai întunecate secrete ale administraţiei, iar lucrul de care se tem ei este lumina.

Edward Joseph Snowden, SSN: [redacted]
Nume de cod CIA „[redacted]"
Număr de Identificare Agenţie: [redacted]
Fost consilier superior | Agenţia de Securitate Naţională a Statelor Unite, sub acoperire corporativă
Fost ofiţer de teren | Agenţia Centrală de Informaţii a Statelor Unite, sub acoperire diplomatică
Fost lector | Agenţia de Informaţii a Armatei Statelor Unite, sub acoperire corporativă

Capitolul 2
Zece zile în Hong Kong

Am ajuns în Hong Kong duminică noaptea, pe 2 iunie. Planul era să ne întâlnim cu Snowden imediat după ce ajungeam la hotel. După ce am primit camera, la hotelul W din exclusivistul district Kowloon, am deschis computerul și l-am căutat pe programul de chat criptat pe care îl foloseam. Așa cum se întâmpla aproape mereu, el era acolo, așteptând.

După ce am schimbat câteva amabilităţi despre zbor, am trecut la detaliile întâlnirii noastre. „Puteţi veni la hotelul meu“, a spus el.

Aceasta a fost prima mea surpriză, să aflu că stă într-un hotel. Încă nu știam de ce este în Hong Kong, dar am presupus la acel moment că era acolo pentru a se ascunde. Mi-l imaginam într-un fel de cocioabă, un apartament ieftin pe care și-l putea permite pentru a se ascunde în lipsa unui salariu regulat, nu instalat confortabil într-un hotel, la vedere, desfășurându-și activitatea zilnică.

Schimbându-ne planurile, am decis că cel mai bine ar fi să așteptăm până dimineaţa pentru a ne întâlni. Snowden a fost cel care a luat decizia, impunând o stare de precauție extremă și mister ce avea să persiste în următoarele zile.

„Veţi atrage mult mai probabil atenţia asupra voastră dacă vă veţi deplasa noaptea“, a spus el. „Este un comportament straniu ca doi americani să se cazeze la hotel noaptea și apoi să iasă imediat. Ar fi mai natural dacă aţi veni aici de dimineaţă.“

Snowden era la fel de îngrijorat de supravegherea de către autorităţile hongkongheze și chineze cât era și de americani. Era foarte preocupat că am putea fi urmăriţi de agenţi de informaţii locali. Presupunând că avusese o relație strânsă cu

agenţiile de spionaj americane și că știe despre ce vorbește, am luat în considerare opinia sa, dar am fost dezamăgit că nu ne putem întâlni în seara respectivă.

Hong Kongul este cu 12 ore înaintea New Yorkului, așa că noaptea și ziua erau acum inversate; abia dacă am dormit în acea noapte, ca de altfel pe toată durata călătoriei. Diferenţa de fus orar a fost doar în parte de vină; într-o stare de surescitare greu controlabilă, am putut să aţipesc doar vreo 90 de minute, două ore cel mult, iar acesta a rămas tiparul meu de somn normal pentru tot sejurul.

În dimineaţa următoare, eu și Laura ne-am întâlnit în lobby și am luat un taxi către hotelul lui Snowden. Laura aranjase detaliile întâlnirii cu el. Era foarte reticentă în a vorbi în taxi, temându-se că șoferul ar putea fi agent sub acoperire. Am respins rapid aceste temeri ca fiind paranoia. În pofida constrângerilor, am scos destule de la Laura pentru a înţelege planul.

Urma să mergem la etajul trei al hotelului lui Snowden, unde se aflau sălile de conferinţe. El a ales o anume sală de conferinţe pentru ceea ce credea că este echilibrul perfect: suficient de izolată pentru a descuraja „traficul uman“ substanţial, așa cum l-a numit el, dar nu atât de obscură și ascunsă încât să atragă atenţia în timp ce așteptam acolo.

Laura mi-a spus că, odată ce vom ajunge la etajul trei, ar trebui să întrebăm primul angajat al hotelului pe care îl întâlnim în apropierea sălii respective dacă există un restaurant deschis. Întrebarea i-ar fi semnalat lui Snowden, care urma să se afle în apropiere, că nu am fost urmăriţi. În interiorul sălii respective urma să așteptăm pe o canapea din apropierea unui „aligator gigantic“ care, a confirmat Laura, era un fel de decoraţiune a sălii mai degrabă decât un animal viu.

Aveam două ore diferite de întâlnire: 10.00 și apoi 10.20. Dacă Snowden nu reușea să ajungă în două minute la prima oră de întâlnire, urma ca noi să părăsim sala și să ne întoarcem mai târziu la a doua oră stabilită, când el ne-ar fi găsit.

„Cum vom ști că este el?“, am întrebat-o pe Laura. Practic nu știam încă nimic despre el, nici vârstă, rasă, aspect fizic sau altceva.

„Va avea un cub Rubik“, a spus ea.

Am râs zgomotos: situaţia părea atât de bizară, atât de extremă și improbabilă. Este un thriller internaţional suprarealist cu acțiunea în Hong Kong, m-am gândit.

Taxiul ne-a lăsat la intrarea în hotelul Mira, care, am remarcat, era situat tot în districtul Kowloon, un cartier foarte comercial plin cu clădiri înalte elegante și magazine șic: mai vizibil nu se putea. Intrând în lobby, am fost și mai surprins: Snowden stătea într-un hotel mare și scump, despre care știam că trebuie să coste câteva sute de dolari pe noapte. De ce, m-am întrebat, cineva care intenţiona să tragă semnalul de alarmă asupra NSA și care avea nevoie ca totul să se desfășoare în mare secret ar fi mers la Hong Kong să se ascundă într-un hotel de cinci stele într-unul dintre cele mai vizibile cartiere din oraș? Însă nu era timp să insist asupra misterului – urma să întâlnesc sursa în câteva minute și probabil să aflu toate răspunsurile.

Ca multe clădiri din Hong Kong, hotelul Mira era de dimensiunile unui sat. Laura și cu mine am petrecut cel puţin 15 minute străbătând holurile pentru a găsi locul de întâlnire. A trebuit să luăm mai multe ascensoare, să trecem peste pasarele interne și să cerem în mod repetat informaţii de orientare. Când am crezut că suntem aproape de sală, am văzut un angajat al hotelului. Cumva stângaci, i-am pus întrebarea ce ţinea loc de cod și am ascultat instrucţiunile despre diversele opţiuni de restaurante.

După o cotitură, am văzut o ușă deschisă și un aligator uriaș, verde, din plastic zăcând pe podea. Așa cum fuseserăm instruiţi, ne-am așezat pe canapeaua care se afla în mijlocul acestei camere de altfel goale, așteptând agitaţi și în liniște. Sala mică părea să nu aibă o funcţie reală, nimeni nu avea motiv să intre, pentru că nu era nimic acolo decât canapeaua

și aligatorul. După cinci minute foarte lungi de stat în liniște, nu a venit nimeni, așa că am plecat și am găsit o altă sală în apropiere unde am așteptat alte 15 minute.

La 10.20 ne-am întors și ne-am așezat din nou lângă aligator, pe canapea, care se afla în faţa peretelui din spate al sălii și a unei oglinzi mari. După două minute, am auzit pe cineva intrând în sală.

În loc să mă întorc să văd cine a intrat, am continuat să mă uit în oglindă, privind reflecţia unui bărbat care se îndrepta spre noi. Abia când era la câţiva pași de canapea m-am întors.

Primul lucru pe care l-am văzut a fost un cub Rubik nerezolvat, învârtindu-se în mâna stângă a bărbatului. Edward Snowden a salutat, dar nu a întins mâna, având în vedere că aranjamentul era ca întâlnirea să pară întâmplătoare. Așa cum plănuiseră, Laura l-a întrebat despre mâncarea din hotel și el a răspuns că este proastă. Dintre toate întorsăturile surprinzătoare din această poveste, momentul întâlnirii noastre s-a dovedit cea mai mare surpriză.

Snowden avea atunci 29 de ani, dar părea cu cel puţin câţiva ani mai tânăr, îmbrăcat într-un tricou alb cu o inscripţie decolorată, jeanși și ochelari de tocilar șic. Avea un pic de barbă, foarte scurtă, dar părea că abia începuse să se bărbierească. În esenţă era bine clădit și avea o postură militară, dar era destul de slab și palid și – ca toţi trei în acel moment – în mod clar rezervat și precaut. Putea fi orice tip puțin tocilar la 20 și ceva de ani care lucrează într-un laborator informatic într-un campus.

La momentul respectiv, nu am putut să coroborez piesele. Fără să mă fi gândit conștient la acest lucru, presupusesem din mai multe motive că Snowden este mai în vârstă, probabil la 50 sau 60 de ani. Mai întâi, având în vedere că avea acces la atât de multe documente sensibile, presupusesem că avea o poziţie superioară în cadrul sistemului de securitate naţională. Dincolo de aceasta, perspectivele și strategiile sale erau invariabil sofisticate și informate, determinându-mă să cred că era un veteran al scenei politice. În ultimul rând, știam că este

pregătit să renunţe la viaţa sa, să își petreacă probabil restul existenței în închisoare, pentru a dezvălui ceea ce simţea el că lumea trebuie să știe, așa că îmi imaginasem că era aproape de sfârșitul carierei. Îmi imaginasem că dacă cineva a ajuns la o decizie atât de extremă, de autosacrificiu, trebuie să fi experimentat mulţi ani, chiar zeci de ani, de dezamăgire profundă.

Să văd că sursa materialelor uimitoare despre NSA era un bărbat atât de tânăr a fost una dintre cele mai debusolante experienţe pe care le-am avut vreodată. Mintea mea a început să analizeze rapid posibilităţile: Era un soi de escrocherie? Mi-am irosit timpul zburând de la un capăt la altul al lumii? Cum putea cineva atât de tânăr să aibă acces la tipul de informaţie pe care o văzuserăm? Cum putea această persoană să fie atât de pregătită și experimentată în spionaj, cum era în mod clar sursa noastră? Poate era fiul sursei, m-am gândit, sau un asistent, sau iubit care urma să ne ducă la sursa însăși. Fiecare posibilitate imaginabilă îmi trecea prin minte și nici una dintre ele nu avea sens.

„Așadar, haideţi cu mine“, a spus el, în mod evident tensionat. Eu și Laura l-am urmat. Am îngăimat cu toţii câteva cuvinte incoerente de politeţe în timp ce mergeam. Eram prea uimit și confuz pentru a spune prea multe și, după cum vedeam, și Laura simţea același lucru. Snowden părea foarte vigilent, ca și cum căuta potenţiali urmăritori sau semne care să indice eventuale probleme. Așa că l-am urmat în mare parte în tăcere.

Fără să avem vreo idee unde ne duce, am intrat în ascensor, am coborât la etajul zece, apoi ne-a condus către camera lui. Snowden a scos un card de acces din portofel și a deschis ușa. „Bine aţi venit“, a spus. „Scuze, e cam dezordine, dar practic nu am părăsit camera de câteva săptămâni.“

Camera era într-adevăr dezordonată, cu farfurii pline pe jumătate cu mâncare de la room-service stivuite pe o masă și haine murdare împrăștiate peste tot. Snowden a eliberat un scaun și m-a invitat să iau loc. El s-a așezat pe pat. Pentru că era o cameră mică, stăteam la mai puţin de un metru și

jumătate unul de celălalt. Conversaţia noastră a fost tensionată, stângace și nenaturală.

Snowden a ridicat imediat problema securităţii, întrebând dacă am telefon mobil. Telefonul meu funcţiona doar în Brazilia, dar Snowden a insistat oricum să îi scot bateria sau să îl pun în frigiderul minibarului său, care ar fi făcut conversaţia mai greu de auzit.

La fel cum îmi spusese și Laura în aprilie, Snowden a afirmat că administraţia americană are capacitatea de a activa de la distanţă telefoane mobile și de a le converti în dispozitive de ascultare. Așa că știam că tehnologia există, dar îngrijorarea lor încă mi se părea vecină cu paranoia. Așa cum s-a dovedit, eu eram cel care se înșela. Administraţia folosise această tactică în anchete penale de ani de zile. În 2006, un judecător federal care prezida o urmărire penală a unui presupus mafiot din New York[1] a decis că folosirea de către FBI a așa-numitelor „roving bugs“ – care transformă propriul telefon mobil al unei persoane în dispozitiv de ascultare prin activarea de la distanţă – este legală.

După ce telefonul meu mobil a fost închis în frigider, Snowden a luat pernele de pe pat și le-a pus în partea de jos a ușii. „Asta e pentru cei care trec prin hol“, a explicat el. „Ar putea fi dispozitive audio sau camere de luat vederi aici, dar oricum ce vom discuta va ajunge în presă“, a declarat el, glumind doar pe jumătate.

Capacitatea mea de a evalua oricare dintre aceste lucruri era foarte limitată. Încă știam foarte puţine despre cine era Snowden, unde lucra, care erau adevăratele lui motive sau ce făcuse, așa că nu puteam fi sigur ce ameninţări ne puteau pândi, în ce privește supravegherea sau de alt fel. Sentimentul meu constant era nesiguranţa.

Fără să se deranjeze să se așeze sau să spună ceva, poate pentru a se elibera de tensiune, Laura a început să își despacheteze camera de luat vederi și trepiedul și să le asambleze. Apoi a venit și ne-a pus microfoane atât lui Snowden, cât și mie.

Discutaserăm planul ei de a ne filma în timp ce ne aflam în Hong Kong: până la urmă era un documentarist care lucra la un film despre NSA. Inevitabil, ceea ce făceam urma să devină o parte uriașă a proiectului ei. Știam acest lucru, dar nu eram pregătit ca înregistrarea să înceapă așa de repede. Îmi era greu să aduc laolaltă în mintea mea cele două lucruri atât de șocante: pe de o parte, întâlnirea secretă cu o sursă care, pentru administraţia americană, comisese infracţiuni grave și, pe de altă parte, filmarea acestui lucru.

Laura a fost gata în câteva minute. „Așadar o să încep să filmez", a anunţat ea, ca și cum era cel mai natural lucru din lume. Conștientizarea faptului că urma să fim filmaţi a amplificat tensiunea.

Acea interacţiune iniţială dintre mine și Snowden era stângace, dar imediat ce camera a început să înregistreze, am devenit amândoi instantaneu mult mai formali și mai puţin prietenoși; postura noastră a devenit rigidă și vorbirea încetinită. De-a lungul anilor, am susţinut multe discursuri despre cum schimbă supravegherea comportamentul uman, evidenţiind studii care arătau că persoanele care știu că sunt privite sunt mult mai limitate, mai precaute în legătură cu ceea ce spun, mai puţin libere. Acum vedeam și simţeam ilustrarea vie a acestei dinamici.

Având în vedere inutilitatea încercărilor noastre de a schimba amabilităţi, nu mai era altceva de făcut decât să trecem direct la subiect. „Am o mulțime de întrebări pentru tine și voi începe pur și simplu să ţi le adresez, una câte una, și, dacă ești de acord, putem aprofunda pe măsură ce discuția înaintează", am început.

„Este în regulă", a spus Snowden, în mod clar la fel de ușurat ca și mine să trecem la subiect.

La acel moment aveam două obiective principale. Pentru că știam cu toţii că exista un risc serios ca el să fie arestat în orice moment, prioritatea mea era să aflu orice puteam despre Snowden: despre viaţa sa, locurile de muncă, ce îl determinase

să facă această alegere extraordinară, ce făcuse mai exact pentru a lua documente și de ce și ce făcea în Hong Kong. În al doilea rând, eram hotărât să îmi dau seama dacă era sincer și complet deschis sau dacă ascundea lucruri importante despre cine era și ce făcuse.

Deși scriam despre politică de aproape opt ani, experienţa mai relevantă pentru ce urma să fac era cariera mea anterioară de avocat pledant, care includea luarea depoziţiilor de la martori. În timpul luării unei depoziţii, avocatul stă la o masă cu un martor ore întregi, uneori zile. Martorul este obligat de lege să fie acolo și să răspundă sincer la orice întrebare a ta. Un obiectiv-cheie este să demaști minciuni, să găsești contradicții în povestea martorului și să pătrunzi dincolo de orice ficţiune creată de martor pentru a lăsa adevărul să iasă la iveală. Luarea de depoziţii a fost unul dintre puţinele lucruri care chiar mi-au plăcut la meseria de avocat și am elaborat tot felul de tactici pentru a afla adevărul de la un martor. Acestea implicau mereu un tir neîncetat de întrebări, adeseori aceeași întrebare adresată în mod repetat, dar în contexte diferite, din alte puncte de vedere, pentru a testa soliditatea poveștii.

Schimbându-mi atitudinea cu Snowden de la cea adoptată online, când am vrut să fiu pasiv și respectuos, astăzi urma să folosesc tactici agresive. Fără prea multe pauze, doar pentru mers la toaletă sau pentru a lua o gustare, am petrecut cinci ore chestionându-l. Am început cu copilăria lui, apoi am continuat cu școala primară, istoricul activităţii sale înainte de cea în slujba administraţiei. L-am întrebat fiecare detaliu pe care și-l putea aminti. După cum am aflat, Snowden se născuse în Carolina de Nord și crescuse în Maryland, fiind fiul unor angajaţi ai administraţiei federale din clasa de mijloc (tatăl lui lucrase pentru Paza de Coastă timp de 30 de ani). Snowden a simţit că îi lipsesc provocările în liceu și nu l-a terminat, fiind mult mai interesat de internet decât de ore.

Aproape imediat, am putut vedea în realitate ceea ce observasem în discuţiile noastre online: Snowden era foarte

inteligent și raţional, iar procesele sale cognitive erau metodice. Răspunsurile sale erau concise, clare și logice. Practic, de fiecare dată erau reacţia directă la ceea ce întrebasem, gândite și deliberate. Nu erau devieri ciudate sau povești improbabile de tipul celor care să semnaleze o persoană instabilă emoţional sau care suferă de afecţiuni psihologice. Stabilitatea și concentrarea sa inspirau încredere.

Deși ne formăm ușor o impresie despre oameni din interacţiunile online, trebuie să ne vedem în persoană pentru a ne da seama cine sunt aceștia. M-am simţit rapid mai bine în situaţia dată, revenindu-mi după îndoielile iniţiale și dezorientarea cu care mă confruntam. Dar încă eram profund sceptic, pentru că știam că tot ceea ce urma să facem, inclusiv credibilitatea noastră, depinde de autenticitatea a ceea ce pretindea Snowden că este.

Am petrecut câteva ore concentrați asupra activităţii sale și a evoluţiei lui intelectuale. Ca mulţi americani, vederile politice ale lui Snowden se schimbaseră semnificativ după atacul din 11 septembrie: a devenit mult mai „patriot". În 2004, la vârsta de 20 de ani, se înrolase în armata SUA pentru a lupta în războiul din Irak, despre care la momentul respectiv credea că este un efort nobil de a elibera poporul irakian de oprimare. După doar câteva săptămâni de antrenament de bază, a văzut că se vorbea mai mult despre uciderea arabilor decât despre eliberarea cuiva. Când și-a fracturat ambele picioare în urma unui accident la antrenament și a fost obligat să renunţe la armată, era deja foarte dezamăgit de scopul real al războiului.

Dar Snowden credea încă în faptul că administraţia Statelor Unite este în esenţă bună, așa că a decis să urmeze exemplul multor membri ai familiei sale și a mers să lucreze pentru o agenţie federală. Fără o diplomă de liceu, a reușit totuși să se descurce ca tânăr adult și să-și creeze oportunităţi, lucrând inclusiv în domeniul tehnic, muncă plătită cu 30 de dolari ora înainte de a împlini 18 ani, și a fost inginer de sistem certificat de Microsoft din 2002. Dar el a văzut o carieră în administraţia

federală ca fiind ceva nobil și totodată promițător din punct de vedere profesional, așa că a început ca agent de pază la Centrul pentru Studii Avansate ale Limbajului la Universitatea Maryland, o clădire administrată și folosită în secret de NSA. Intenția, a spus el, era să poată fi verificat și astfel să facă primul pas pentru a trece apoi la o muncă tehnică.

Deși Snowden a abandonat liceul, avea un talent natural pentru tehnologie, ceea ce a devenit evident încă din primii săi ani de adolescență. Alături de inteligența sa evidentă, aceste atribute, în pofida vârstei sale fragede și a lipsei de educație formală, i-au permis să avanseze rapid în carieră, trecând repede de la agent de pază la o poziție de expert tehnic pentru CIA în 2005.

A explicat că întreaga comunitate de spionaj era disperată după angajați cu competențe tehnice. Se transformase într-un sistem atât de vast, încât găsirea unor oameni capabili să îl opereze era dificilă. Astfel, agențiile de securitate națională au fost nevoite să se întoarcă spre pepiniere de talente netradiționale pentru a recruta. Persoanele cu abilități informatice suficient de avansate sunt mai degrabă tinere și deseori alienate și adesea au eșuat în a străluci în sistemul educațional. Ele consideră deseori cultura internetului mult mai stimulativă decât instituțiile educaționale oficiale și interacțiunile personale. Snowden a devenit un membru valoros al acestei echipe IT la agenție, în mod clar mai cunoscător și mai competent decât majoritatea colegilor săi mai în vârstă și cu educație superioară. Snowden a simțit că a găsit exact mediul în care competențele sale vor fi răsplătite și lipsa lui de calificare academică ignorată.

În 2006 a făcut tranziția de la o persoană aflată sub contract cu CIA la angajat cu normă întreagă, ceea ce i-a sporit oportunitățile pe viitor. În 2007 a aflat despre un loc de muncă la CIA care presupunea lucrul la sisteme informatice din străinătate. Obținând recomandări strălucite de la șefii săi, a primit locul de muncă și a sfârșit prin a lucra pentru CIA

în Elveţia. A fost staţionat în Geneva timp de trei ani, până în 2010, aflându-se sub acoperire, cu acreditări diplomatice.

Așa cum și-a descris Snowden activitatea la Geneva, a fost mai mult decât un simplu „administrator de sistem". A fost considerat principalul expert tehnic și în securitate informatică din Elveţia, a primit ordin să călătorească în toată regiunea și să rezolve probleme pe care nimeni altcineva nu le putea rezolva. A fost ales de CIA să acorde asistență președintelui la summitul NATO din 2008 din România. În pofida acestui succes, tocmai în timpul detașării sale în cadrul CIA a început Snowden să se simtă tulburat de acţiunile administraţiei.

„Deoarece experţii tehnici au acces la sistemele de computere, am văzut multe lucruri secrete", mi-a spus Snowden, „și multe dintre ele arătau destul de rău. Am început să înţeleg că ce face cu adevărat guvernul meu în lume este foarte diferit de ceea ce crezusem eu. Această descoperire te face să începi să reevaluezi modul în care privești lucrurile, să pui mai multe întrebări".

Un exemplu pe care l-a amintit el a fost o încercare a unor ofiţeri de caz CIA de a recruta un bancher elveţian pentru a furniza informaţii confidenţiale. Ei voiau să știe despre tranzacţiile financiare ale persoanelor de interes pentru Statele Unite. Snowden a povestit cum unul dintre ofiţerii sub acoperire s-a împrietenit cu bancherul, l-a îmbătat într-o noapte și l-a încurajat să conducă mașina până acasă. Când bancherul a fost oprit de poliţie și arestat pentru conducere sub influenţa alcoolului, agentul CIA s-a oferit să îl ajute personal în diverse moduri, cu condiţia ca bancherul să coopereze cu agenţia. Efortul de recrutare a eșuat în cele din urmă. „Au distrus viaţa ţintei pentru ceva ce nici măcar nu a mers, după care au plecat pur și simplu", a spus el. Dincolo de schemă în sine, Snowden era tulburat și de modul în care agentul se lăudase cu metodele folosite pentru a-l prinde în cursă pe bancher.

Un element care a amplificat frustrarea a venit din eforturile lui Snowden de a le atrage atenţia superiorilor săi în legătură

cu problemele de securitate informatică sau sistemele informatice despre care el credea că depășesc limitele etice. Aceste eforturi, a spus el, au fost aproape întotdeauna respinse.

„Spuneau că nu este treaba ta sau ţi se spunea că nu ai suficiente informaţii pentru a face astfel de judecăţi. Practic erai instruit să nu îţi faci griji în această privinţă“, a spus el. Și-a câștigat printre colegi reputaţia unei persoane excesiv de preocupate, o trăsătură care nu l-au făcut prea îndrăgit de superiori. „Atunci am început cu adevărat să văd cât de ușor este să desparţi puterea de responsabilitate și că, cu cât nivelurile de putere erau mai înalte, cu atât supravegherea și responsabilitatea erau mai mici.“

Spre sfârșitul lui 2009, Snowden, care era deja dezamăgit, a decis că este gata să părăsească CIA. În acel moment, la sfârșitul detașării sale la Geneva, a început să se gândească prima oară la posibilitatea de a deveni un avertizor de integritate și de a fi sursa unor scurgeri de informaţii secrete despre care el credea că dovedesc neregulile.

„De ce nu ai făcut-o atunci?“, am întrebat.

La momentul respectiv credea sau cel puţin spera că alegerea lui Barack Obama la președinţie va reforma unele dintre cele mai grave abuzuri pe care le văzuse. Obama și-a început mandatul promiţând să schimbe abuzurile excesive din cadrul securităţii naţionale care fuseseră justificate de războiul împotriva terorismului. Snowden se aștepta ca măcar unele dintre neregulile cele mai mari din lumea serviciilor de spionaj și din cea militară să fie rezolvate.

„Dar apoi a devenit clar că Obama nu numai că le continua, ci în multe cazuri extindea aceste abuzuri“, a spus el. „Mi-am dat seama atunci că nu mai pot aștepta ca un lider să rezolve aceste lucruri. Leadershipul înseamnă ca mai întâi să acţionezi și să servești ca exemplu pentru alţii, nu să aștepţi ca alţii să acţioneze.“

Era, de asemenea, îngrijorat în legătură cu prejudiciile care ar rezulta din dezvăluirea a ceea ce aflase la CIA. „Când

dai publicităţii secrete ale CIA, poţi răni oameni“, a spus el, referindu-se la agenţi sub acoperire și informatori. „Nu voiam să fac acest lucru. Dar atunci când dai publicităţii secrete ale NSA, faci rău doar sistemului abuziv. Mă simţeam mult mai relaxat din acest punct de vedere.“

Așa că Snowden s-a întors la NSA, de această dată ca să lucreze pentru Dell Corporation, care avea contract cu agenţia. În 2010, se afla în Japonia și i se oferise un acces mult mai mare la secretele supravegherii decât anterior.

„Lucrurile pe care le-am văzut chiar au început să mă tulbure“, a spus Snowden. „Puteam să văd drone în timp real când supravegheau persoane pe care trebuiau să le ucidă. Puteai urmări un întreg sat și vedea ce face fiecare. Am văzut NSA în timp ce urmărea activităţile pe internet ale unor persoane când tastau. Am devenit conștient de cât de invazive deveniseră capacităţile de supraveghere ale SUA. Am realizat adevărata amploare a acestui sistem. Și aproape nimeni nu știa ce se întâmplă.“

Nevoia resimţită, *obligaţia* de a da publicităţii ceea ce vedea devenea tot mai urgentă pentru el. „Cu cât petreceam mai mult timp la NSA în Japonia, cu atât mai mult știam că nu pot păstra aceste lucruri doar pentru mine. Am simţit că ar fi greșit, de fapt, să ajut la ascunderea tuturor acestor lucruri de public.“

Mai târziu, după ce identitatea lui Snowden a fost dezvăluită, reporterii au încercat să îl descrie ca naiv, un individ de nivel inferior în IT, care se întâmplase să dea peste informaţii clasificate. Dar realitatea era cu mult diferită.

Pe tot parcursul activităţii sale la CIA și NSA, mi-a spus Snowden, a fost antrenat progresiv să devină un operator informatic de nivel înalt, o persoană care să intre neautorizată în sistemele militare și civile ale altor ţări, să fure informaţii sau să pregătească atacuri fără a lăsa urme. În Japonia, această formare s-a intensificat. A aprofundat cele mai sofisticate metode de protejare a datelor electronice de alte agenţii de informaţii și a fost certificat oficial ca operator informatic de nivel

înalt. În cele din urmă a fost ales de Academia de Pregătire în Contraspionaj a Agenţiei de Informaţii Militare pentru a preda contraspionaj cibernetic în cadrul cursului lor de contraspionaj chinez.

Metodele de securitate operaţionale pe care a insistat el să le urmăm erau unele pe care le învăţase și la a căror concepere chiar ajutase în cadrul CIA și mai ales al NSA.

În iulie 2013, *New York Times* a confirmat[2] ceea ce mi-a spus Snowden, relatând că „în timp ce lucra pentru un contractant al Agenţiei de Securitate Naţională, Edward J. Snowden a învăţat să fie hacker“ și că „s-a transformat în genul de expert în securitate informatică pe care NSA este disperată să îl recruteze“. Formarea pe care a primit-o acolo, afirmă *New York Times*, a fost „crucială în orientarea sa către securitatea informatică mult mai sofisticată“. Articolul adăuga că fișierele pe care le-a accesat Snowden au arătat că el „s-a orientat către partea ofensivă a spionajului electronic sau războiul cibernetic, în care NSA examinează sistemele informatice ale altor naţiuni pentru a fura informaţii sau pentru a pregăti atacuri“.

Deși am încercat să urmăresc o cronologie în întrebările mele, de multe ori nu am rezistat să fac salturi înainte, în mare parte din cauza nerăbdării. În special am vrut să ajung la nucleul a ceea ce, pentru mine, a fost cel mai uluitor mister de când am început să vorbesc cu el: ce l-a determinat cu adevărat pe Snowden să renunţe la cariera lui, să se transforme el însuși într-un potenţial trădător și să încalce regulile de discreţie și loialitate care i-au fost repetate insistent ani la rând?

I-am pus aceeași întrebare în feluri diferite, iar Snowden a răspuns, așadar, în moduri diferite, dar explicaţiile au fost fie prea superficiale, fie prea abstracte, fie prea lipsite de pasiune și convingere. Se simţea foarte confortabil vorbind despre sistemele NSA și tehnologie, dar mai puţin confortabil când el însuși era subiectul, în special în răspunsul la sugestia că a făcut ceva curajos și extraordinar care garanta o explicaţie psihologică. Răspunsurile lui au părut mai mult abstracte

decât viscerale, așa că le-am considerat neconvingătoare. Lumea trebuie să știe ce s-a făcut cu dreptul său la viaţă privată, a spus el; a simţit o obligaţie morală de a lua act împotriva neregulilor; nu era împăcat cu sine dacă păstra tăcerea în legătură cu ameninţarea ascunsă la adresa valorilor pe care el le preţuia.

Cred că aceste valori politice erau reale pentru el, dar voiam să știu ce îl determinase pe el personal să își sacrifice viaţa și libertatea pentru apărarea acestor valori și am simţit că nu primesc răspunsul real. Poate că nu avea acest răspuns sau poate, la fel ca mulţi americani, mai ales când sunt afundaţi într-o cultură a securităţii naţionale, era reticent în a săpa prea adânc în psihicul său, dar trebuia să aflu.

Dincolo de orice altceva, voiam să fiu sigur că făcuse această alegere înţelegând cu adevărat și raţional consecinţele; nu voiam să-l ajut să își asume un risc atât de mare decât dacă eram convins că face acest lucru în mod autonom și activ, înţelegându-și cu adevărat scopul.

În cele din urmă, Snowden mi-a dat un răspuns pe care l-am simţit vibrant și real. „Adevărata măsură a valorii unei persoane nu stă în ceea ce spune că sunt convingerile sale, ci în ceea ce face în apărarea acestor convingeri", a spus el. „Dacă nu acţionezi în numele convingerilor tale, atunci probabil că acestea nu sunt reale."

Cum ajunsese el la această unitate de măsură pentru aprecierea propriei valori? De unde dobândise această credinţă că putea să acţioneze moral doar dacă era dispus să își sacrifice propriile interese pentru un bine mai mare?

„Din multe locuri diferite, o mulţime de experienţe", a spus Snowden. Crescuse citind mult din mitologia greacă și fusese influenţat de cartea *The Hero with a Thousand Faces (Eroul cu o mie de chipuri)* a lui Joseph Campbell, care, a subliniat el, „găsește puncte comune între poveștile pe care le împărtășim cu toţii". Principala lecţie din această carte a fost că „noi suntem cei care impregnăm sens vieţii prin acţiunile noastre

și poveștile pe care le creăm cu ele“. Oamenii sunt definiţi doar de acţiunile lor. „Nu vreau să fiu o persoană căreia să îi fie frică să acţioneze pentru apărarea principiilor sale“.

Această temă, acest construct moral de evaluare a identităţii și valorii cuiva el l-a întâlnit în mod repetat pe parcursul evoluţiei sale intelectuale, inclusiv, după cum a explicat cu o ușoară jenă, în jocurile video. Lecţia pe care a învăţat-o din cufundarea în jocurile video, a spus el, a fost că o singură persoană, chiar și cea mai lipsită de putere, poate înfrunta marea nedreptate. „Protagonistul este deseori o persoană obișnuită, care se confruntă cu nedreptăţi grave din partea unor forţe puternice și poate să aleagă între a fugi de teamă sau a lupta pentru convingerile sale. Iar istoria arată că aceiași oameni obișnuiţi care sunt suficient de hotărâţi să obţină dreptatea pot triumfa în faţa celor mai de temut adversari.“

Nu a fost prima persoană pe care am auzit-o afirmând că jocurile video au contribuit la formarea viziunii proprii despre lume. Poate voi fi luat în derâdere, dar, cu ani în urmă, am ajuns să accept că, pentru generaţia lui Snowden, ele au jucat un rol la fel de serios în modelarea conștiinţei politice, a gândirii etice și a înţelegerii locului cuiva în lume ca literatura, televiziunea și filmul. Și ele, de multe ori, prezintă dileme morale complexe și provoacă la meditaţie, mai ales în cazul persoanelor care au început să pună la îndoială cele învăţate.

Concepţia etică timpurie a lui Snowden – rezultată din activitatea care a constituit, așa cum spune el, „un model pentru cine vrem să devenim și de ce“ – a evoluat către o introspecţie adultă serioasă în legătură cu obligaţiile etice și limitele psihologice. „Ceea ce menţine o persoană pasivă și supusă“, a explicat el, este „teama acesteia de repercusiuni, dar odată ce te eliberezi de atașamentul faţă de lucruri care în cele din urmă nu contează – bani, carieră, siguranţă fizică –, poţi depăși această frică“.

La fel de centrală în viziunea lui despre lume era și valoarea fără precedent a internetului. Ca pentru mulţi din generaţia

sa, „internetul“ nu era un instrument izolat de folosit pentru sarcini discrete. Era lumea în care mintea și personalitatea lui s-au dezvoltat, un loc către sine care a oferit libertate, explorare și potențial pentru dezvoltarea intelectuală și înțelegere.

Pentru Snowden, calitățile unice ale internetului erau de o valoare fără termen de comparație, ele trebuind păstrate cu orice preț. A folosit internetul ca adolescent pentru a explora idei și pentru a vorbi cu oameni din locuri îndepărtate și cu un trecut radical diferit, pe care altfel nu i-ar fi întâlnit. „În esență, internetul mi-a permis să experimentez libertatea și să îmi explorez capacitatea deplină ca ființă umană.“ Animat în mod clar și chiar pasionat când a vorbit despre valoarea internetului, Snowden a adăugat că „pentru mulți copii, internetul este un mijloc de autocunoaștere. Le permite să exploreze cine sunt și cine vor să fie, dar acest lucru funcționează doar dacă putem rămâne în intimitate și anonimi, pentru a face greșeli fără ca ei să ne urmărească. Mă tem că generația mea a fost ultima care s-a bucurat de această libertate“.

Rolul pe care aceasta l-a jucat în decizia lui a devenit clar pentru mine. „Nu vreau să trăiesc într-o lume în care nu avem intimitate și libertate, în care singura valoare a internetului este spulberată“, mi-a spus Snowden. În consecință, s-a simțit obligat să facă tot posibilul pentru a împiedica acest lucru să se întâmple sau, mai exact, pentru a le permite altora să aleagă dacă acționează sau nu în apărarea acestor valori.

Snowden a subliniat în mod repetat că scopul său nu era să distrugă capacitatea NSA de a elimina intimitatea. „Nu este rolul meu să fac această alegere“, a spus el. În schimb, el a vrut ca americanii și oamenii din lumea întreagă să știe ce s-a făcut cu intimitatea lor, să le ofere informația. „Nu intenționez să distrug aceste sisteme“, a insistat el, „ci să permit publicului să decidă dacă ele ar trebui să continue“.

Deseori, avertizorii de integritate ca Snowden sunt demonizați ca singuratici sau ratați, oameni care nu acționează din conștiință, ci din alienare și frustrare față de viața lor eșuată.

Snowden era opusul: el a avut o viaţă plină cu aceste lucruri pe care oamenii le văd ca fiind cele mai de preţ. Decizia sa de a da publicităţii aceste documente însemna renunţarea la o iubită pe care o avea de multă vreme, la o viaţă în paradisul hawaiian, la o familie care l-a susţinut mereu, la o carieră stabilă, un salariu mare, o perspectivă plină de oportunități.

După ce detașarea NSA a lui Snowden în Japonia s-a încheiat în 2011, el a mers să lucreze din nou pentru Dell Corporation, de data aceasta la un birou CIA din Maryland. Împreună cu bonusurile primite, era pe cale să ajungă la suma de 200 000 de dolari în acel an, lucrând cu Microsoft și alte companii tehnologice ca să pună la punct un sistem sigur pentru CIA și alte agenţii pentru ca acestea să își arhiveze documentele și datele. „Situaţia se înrăutăţea", a declarat Snowden despre perioada respectivă. „Din poziţia pe care o deţineam, am văzut la sursă că statul, în special NSA, lucra mână în mână cu industria tehnologică privată pentru a primi acces deplin la comunicaţiile oamenilor."

În cinci ore de interviu în acea zi – de fapt tot timpul cât am vorbit cu el în Hong Kong –, tonul lui Snowden a fost aproape mereu stoic, calm, realist. Dar când a explicat ce a descoperit, lucrul care l-a determinat în cele din urmă să treacă la acţiune, a devenit însufleţit, chiar ușor agitat. „Mi-am dat seama", a spus el, „că ei construiau un sistem ale cărui scopuri erau să elimine intimitatea, și aceasta la nivel global. Să facă în așa fel încât nimeni să nu mai comunice electronic fără ca NSA să fie capabilă să colecteze, să depoziteze și să analizeze acea comunicare".

Conștientizarea acestui fapt i-a întărit hotărârea de a deveni avertizor de integritate. În 2012, el a fost transferat de Dell din Maryland în Hawaii. A petrecut o parte din anul 2012 descărcând documente despre care credea că lumea ar trebui să le vadă. A luat alte documente nu pentru publicare, ci pentru ca jurnaliștii să poată înţelege contextul sistemului despre care scriau.

La începutul lui 2013 și-a dat seama că exista un set de documente necesar pentru a completa imaginea pe care voia să o prezinte lumii, documente la care nu avea acces de la Dell. Acestea erau accesibile doar dacă obţinea o poziţie diferită, una în care să fie desemnat oficial ca analist de infrastructură, ce îi permitea să pătrundă în tot depozitul de supraveghere brută al NSA.

Urmărind acest obiectiv, Snowden și-a depus candidatura pentru un job în Hawaii la Booz Allen Hamilton, una dintre cele mai mari și mai puternice firme contractante din domeniul apărării, la care lucrau numeroși foști oficiali guvernamentali. Salariul i s-a redus pentru acest post, dar a primit acces la descărcarea ultimului set de fișiere de care simţea că are nevoie pentru a completa imaginea spionajului NSA. Cel mai important era faptul că accesul îi permitea să strângă informaţii despre monitorizarea secretă desfășurată de NSA în cazul întregii infrastructuri de telecomunicaţii din SUA.

La jumătatea lui mai 2013, Snowden a cerut să i se dea câteva săptămâni libere pentru a se trata de epilepsie, boală de care descoperise că suferă cu un an înainte. Și-a făcut bagajele, inclusiv câteva dispozitive de stocare pline cu documente NSA, alături de patru laptopuri goale pentru diverse scopuri. Nu i-a spus iubitei lui unde merge; de fapt era ceva obișnuit pentru el să călătorească în interes de serviciu fără să îi poată spune destinaţia. Voia ca aceasta să nu știe de planurile lui, pentru a evita ca ea să fie expusă hărţuirii guvernamentale odată ce identitatea lui va fi dezvăluită.

A ajuns la Hong Kong din Hawaii la 20 mai, cazându-se la hotelul Mira cu numele său real.

Snowden stătea la hotel fără să se ascundă, plătind cu cardul de credit pentru că, a explicat el, știa că mișcările sale vor fi în cele din urmă examinate cu atenţie de administraţie, de presă și de toţi ceilalţi. Voia să prevină orice afirmaţie cum că ar fi vreun agent străin, care ar fi fost mai ușor de făcut dacă și-ar fi petrecut această perioadă ascuns. Voia să demonstreze

că mișcările sale pot fi verificate, că nu există nici o conspirație și că a acționat singur. Pentru autoritățile din Hong Kong și China, el părea un om de afaceri obișnuit, nu o persoană care se ascunde. „Nu intenționez să ascund cine sau ce sunt“, a spus el, „așa că nu am nici un motiv să mă ascund și să alimentez teoriile conspirației sau campaniile de demonizare“.

Apoi i-am pus întrebarea pe care o aveam în minte de prima dată când am vorbit online: de ce alesese Hong Kong ca destinație, de vreme ce era pregătit să dezvăluie documentele? În mod caracteristic, răspunsul lui Snowden a arătat că decizia se bazase pe o analiză atentă.

Principala lui prioritate a fost să își garanteze siguranța fizică față de interferența Statelor Unite în timp ce lucra cu Laura și cu mine la documente. Dacă autoritățile americane descopereau planul lui de a publica documentele, ar fi încercat să îl oprească, arestându-l sau mai rău. Hong Kong, deși semi-independent, face parte din teritoriul Chinei, a argumentat el, iar agenților americani le-ar fi mai greu să opereze împotriva lui aici decât în alte locuri la care se gândise el ca ultim refugiu, cum ar fi o țară mică din America Latină precum Ecuador sau Bolivia. Hong Kongul ar fi totodată mai capabil și mai doritor să reziste în fața presiunii SUA de a-l preda decât o națiune europeană mică, cum ar fi Islanda.

Deși aducerea documentelor în fața publicului a fost principala preocupare în alegerea destinației, aceasta nu a fost și singura. El voia, de asemenea, să fie într-un loc unde oamenii să fie dedicați unor valori politice importante pentru el. Așa cum a explicat, populația din Hong Kong, deși supusă unei legi represive de către guvernul chinez, a trebuit să lupte pentru păstrarea unor libertăți politice elementare și să creeze un climat vibrant de dezaprobare. Snowden a subliniat că Hong Kongul și-a ales liderii în mod democratic și a fost teatrul unora dintre cele mai mari proteste stradale, inclusiv un marș anual împotriva reprimării mișcării din Piața Tiananmen.

Au fost și alte locuri în care ar fi putut merge, care i-ar fi oferit o protecţie chiar și mai mare faţă de o potenţială acţiune a SUA, inclusiv China continentală. Și erau, cu siguranţă, ţări care se bucurau de mai multă libertate politică. El a simţit însă că Hong Kongul oferă cea mai bună combinație de securitate fizică și putere politică.

Cu siguranţă au fost și dezavantaje în cazul acestei decizii, iar Snowden era conștient de toate, inclusiv relaţia orașului cu China continentală, care le-ar fi oferit criticilor o cale mai ușoară de a-l demoniza. Dar nu există alegeri perfecte. „Toate opţiunile mele sunt proaste", a spus el deseori, iar Hong Kongul i-a oferit într-adevăr o oarecare securitate și libertate de mișcare care ar fi fost greu de obţinut în altă parte.

Acum, că aflasem toate datele poveștii, mai aveam un scop: să fiu sigur că Snowden înţelegea ce putea să se întâmple cu el odată ce își va face cunoscută identitatea ca fiind sursa din spatele dezvăluirilor.

Administraţia Obama a dus ceea ce persoanele din spectrul politic numesc un război fără precedent împotriva avertizorilor de integritate. Președintele, care a făgăduit în timpul campaniei electorale că va avea „cea mai transparentă administraţie din istorie", promiţând în mod specific să protejeze avertizorii de integritate, pe care i-a lăudat ca fiind „nobili" și „curajoși", a făcut exact opusul.

Administraţia Obama a acuzat mai mulţi informatori în baza Legii privind Spionajul din 1917 – șapte în total – decât toate administraţiile precedente din istoria SUA *împreună*: de fapt, mai mult decât dublu în total. Legea privind Spionajul a fost adoptată în timpul Primului Război Mondial pentru a-i permite lui Woodrow Wilson să incrimineze opoziţia faţă de război, iar sancţiunile sale sunt dure: ele includ închisoare pe viaţă și chiar pedeapsa cu moartea.

Fără îndoială, greutatea legii l-ar fi zdrobit pe Snowden. Departamentul de Justiţie din administraţia Obama l-ar fi

acuzat de infracţiuni care l-ar fi trimis în închisoare pe viaţă și se putea aștepta să fie denunţat ca trădător.

„Ce crezi că se va întâmpla cu tine odată ce vei dezvălui că tu ești sursa?“, l-am întrebat.

Snowden a răspuns rapid într-un mod care arăta clar că se gândise la această întrebare de multe ori înainte: „Vor spune că am încălcat Legea privind Spionajul. Că am comis infracţiuni grave. Că am ajutat inamicii Americii. Că am periclitat securitatea naţională. Sunt sigur că vor folosi fiecare incident din trecutul meu și probabil îl vor exagera sau vor inventa altele, pentru a mă discredita cât mai mult posibil“.

Nu voia să meargă la închisoare, a spus el. „Voi încerca să evit acest lucru. Dar dacă acesta va fi rezultatul, și știu că există o posibilitate uriașă ca acesta să fie, am decis cu ceva vreme în urmă că pot trăi împăcat cu orice îmi vor face. Singurul lucru cu care nu pot trăi este să știu că nu am făcut nimic.“

În acea primă zi și în fiecare din zilele care au urmat, hotărârea lui Snowden și contemplarea calmă a ceea ce putea să i se întâmple au fost profund surprinzătoare și emoţionante. Nu l-am văzut niciodată arătând regret sau teamă sau anxietate. A explicat fără să clipească faptul că făcuse o alegere, înţelesese posibilele consecinţe și era pregătit să le accepte.

Snowden părea să își tragă puterea din această decizie. Degaja un echilibru mental extraordinar atunci când vorbea despre ce putea să îi facă administraţia americană. Vederea acestui tânăr de 29 de ani care răspundea în acest fel la ameninţarea cu decenii de detenţie sau detenţie pe viaţă într-o închisoare de maximă securitate – o perspectivă care, prin ea însăși, ar fi speriat pe oricine până la paralizie – era profund stimulativă. Iar curajul lui era contagios: eu și Laura ne-am promis în mod repetat unul altuia și lui Snowden că orice acţiune vom întreprinde și orice decizie vom lua o vom face pentru a-i respecta alegerea. Am simţit o datorie de a relata povestea în spiritul care a animat actul iniţial al lui Snowden: curajul înrădăcinat în convingerea că faci ceea ce crezi că este corect

și refuzul de a te lăsa intimidat sau descurajat de amenințări lipsite de fundament din partea unor oficiali răuvoitori dornici să își ascundă propriile acțiuni.

După cinci ore de intervievare eram convins că tot ce spunea Snowden era adevărat și că motivele lui erau chibzuite și reale. Înainte de a pleca de la el, a revenit la subiectul asupra căruia stăruise de mai multe ori: a insistat să se identifice cu sursa documentelor și să o facă public în primul articol pe care îl publicam. „Oricine face ceva atât de semnificativ are obligația să explice publicului de ce a făcut acest lucru și ce speră să obțină“, a spus el. Nu voia ca, ascunzându-se, să amplifice climatul de teamă pe care administrația americană îl crease.

În plus, Snowden era sigur că NSA și FBI vor identifica rapid sursa scurgerii de informații odată ce articolele vor începe să apară. Nu luase toate măsurile posibile pentru a-și acoperi urmele pentru că voia să evite o situație în care colegii lui erau supuși investigațiilor sau unor acuzații false. A insistat că, folosindu-și abilitățile dobândite și având în vedere sistemul NSA incredibil de lax, ar fi putut să își acopere urmele dacă ar fi vrut, chiar descărcând atât de multe documente secrete precum făcuse el. Dar alesese să lase cel puțin unele urme electronice pentru a fi descoperit, ceea ce însemna că rămânerea lui în anonimat nu mai era o opțiune.

Deși nu voiam să ajut administrația să afle identitatea sursei mele dezvăluindu-i-o, Snowden m-a convins că descoperirea identității sale era inevitabilă. Mai important era faptul că era hotărât să se definească în ochii publicului el însuși, mai degrabă decât să lase administrația să îl definească.

Teama lui Snowden despre divulgarea identității lui era că aceasta va distrage de la substanța dezvăluirilor sale. „Știu că presa personalizează totul și că administrația va vrea ca subiectul să fiu eu, pentru a ataca mesagerul“, a spus el. Planul lui era să își divulge identitatea la început, iar apoi să dispară pentru a permite ca lumea să rămână concentrată pe NSA și pe activitățile de spionaj. „Odată ce mă voi identifica și mă voi

explica“, a spus el, „nu voi mai apărea în presă. Nu vreau ca eu să fiu subiectul.“

Am argumentat că mai degrabă decât să dezvăluim identitatea lui Snowden în primul articol, am putea să așteptăm o săptămână, astfel încât să putem relata primul set de informaţii fără vreo distragere a atenţiei de la ele. Ideea noastră era simplă: să relatăm subiecte uriașe unul după altul, în fiecare zi, o versiune jurnalistică de șoc și groază, începând cât mai repede posibil și culminând cu dezvăluirea sursei noastre. La finalul întâlnirii noastre din prima zi, eram cu toţii de acord; aveam un plan.

În restul timpului petrecut în Hong Kong m-am întâlnit și am vorbit zilnic cu Snowden pe larg. Nu am dormit mai mult de două ore pe noapte și acest lucru a fost posibil doar graţie folosirii unor pastile. Restul timpului l-am petrecut scriind articole bazate pe documentele lui Snowden și, odată ce au început să fie publicate, dând interviuri și discutând despre ele.

Snowden ne-a lăsat pe Laura și pe mine să decidem ce subiecte ar trebui relatate, în ce ordine și cum vor fi prezentate. Însă în prima zi – așa cum făcuse de mai multe ori înainte, dar și ulterior – Snowden a subliniat cât de important este să examinăm cu atenţie toate materialele. „Am selectat aceste documente în funcţie de interesul public“, ne-a spus el, „dar mă bazez pe tine să îţi folosești raţionamentul jurnalistic pentru a publica doar documentele pe care publicul ar trebui să le vadă și care pot fi dezvăluite fără să le facă rău oamenilor nevinovaţi“. Snowden știa că posibilitatea de a genera o dezbatere publică reală presupunea să nu permitem administraţiei americane să afirme în mod justificat că am pus în pericol vieţi prin publicarea acestor documente.

El a subliniat, de asemenea, că este vital să publicăm documentele în stil jurnalistic – ceea ce însemna să colaborăm cu presa și să scriem articole care să ofere contextul pentru materiale, și nu să le publicăm în bloc. Această abordare,

credea el, ar oferi mai multă protecţie legală și, mai important, ar permite publicului să asimileze dezvăluirile într-un mod mai ordonat și mai raţional. „Dacă voiam ca documentele să fie distribuite în masă pe internet, aș fi putut să fac acest lucru singur“, a spus el. „Vreau să te asiguri că aceste subiecte sunt tratate unul câte unul, astfel încât oamenii să poată înţelege ceea ce ar trebui să știe.“ Am fost de acord cu toţii să prezentăm documentele în acest mod.

De câteva ori, Snowden a explicat că vrea ca Laura și cu mine să ne implicăm în subiecte de la început pentru că știa că le vom relata agresiv și nu vom fi impresionaţi de ameninţările administraţiei. El s-a referit frecvent la *New York Times* și la alte mijloace de informare majore care nu au publicat subiecte importante la solicitarea administraţiei. Dar, în afară de faptul că voia o relatare agresivă, el voia și jurnaliști meticuloși care să își acorde suficient timp pentru a se asigura că faptele relatate sunt inatacabile și că toate articolele vor fi verificate cu atenţie. „Unele dintre documentele pe care vi le dau nu sunt pentru publicare, ci pentru ca voi să înţelegeţi mai bine cum funcţionează sistemul, astfel încât să puteţi relata corect.“

După prima mea zi plină în Hong Kong, am plecat din camera de hotel a lui Snowden, m-am întors în camera mea și am stat treaz toată noaptea ca să scriu patru articole, sperând că *Guardian* va începe să le publice imediat. Ne aflam sub presiunea timpului: aveam nevoie ca Snowden să revizuiască împreună cu noi cât mai multe documente posibil înainte de a deveni, într-un fel sau altul, inabordabil.

Mai era și un alt motiv de presiune. În taxiul pe drumul către aeroportul JFK, Laura îmi spusese că a vorbit cu câteva publicaţii importante și cu câţiva reporteri despre documentele lui Snowden.

Printre ei se afla și Barton Gellman, de două ori câștigător al Premiului Pulitzer, care fusese în echipa *Washington Post* și care acum colabora cu ziarul ca jurnalist independent. Laura avusese dificultăţi în a convinge unele persoane să meargă cu

ea la Hong Kong, dar Gellman, care era interesat de multă vreme de problemele legate de supraveghere, se arătase interesat.

La recomandarea Laurei, Snowden a fost de acord să i se dea „unele documente“ lui Gellman, cu intenţia ca el și *Post*, împreună cu Laura, să relateze despre unele dezvăluiri.

L-am respectat pe Gellman, dar nu și *Washington Post*, care pentru mine reprezintă mass-media subordonată administrației, întruchipând toate atributele rele ale presei politice americane: apropierea excesivă de guvern, veneraţia faţă de instituţiile de securitate naţională ale statului, excluderea din start a vocilor care nu sunt de acord. Un alt critic al cotidianului, Howard Kurtz, a documentat în 2004 modul în care ziarul a amplificat sistematic vocile care susţineau războiul[3] înaintea invadării Irakului, în timp ce minimaliza sau excludea opoziţia. Modul în care a prezentat *Washington Post* subiectul, a conchis Kurtz, a fost „în mod izbitor subiectiv“, în favoarea invaziei. Pagina editorială a *The Post* a rămas una dintre cele mai vocale și mai absurde voci care au lăudat militarismul SUA, secretul și supravegherea în America.

Cotidianului i s-a oferit un subiect major pentru care nu a făcut nimic să îl obţină și în condiţiile în care sursa – Snowden – nu l-a selectat (dar a acceptat, la recomandarea Laurei). Într-adevăr, prima mea discuţie criptată cu Snowden a avut loc în urma nemulţumirii sale faţă de modul de abordare dominat de teamă al *The Post*.

Una dintre cele câteva critici ale mele în legătură cu WikiLeaks de-a lungul anilor a fost că și ei au oferit la momentul respectiv subiecte majore unor organizaţii media apropiate aparatului de stat, care a făcut tot ce a putut pentru a proteja administraţia, sporindu-și astfel valoarea și importanţa. Subiectele exclusive despre documente strict secrete cresc statutul publicaţiei și îi fac mai puternici pe jurnaliștii care le comunică. E mai firesc să oferi aceste subiecte unor jurnaliști și organizaţii media independenţi, amplificându-le astfel vocile, făcându-i mai vizibili și maximizând impactul lor.

Și mai rău, știam că *The Post* va respecta cu sfinţenie regulile nescrise care guvernează modul în care ziarul relatează despre secrete oficiale. În conformitate cu aceste reguli, care permit administraţiei să controleze dezvăluirile și să minimizeze, chiar să neutralizeze impactul lor, redactorii merg mai întâi la oficiali și îi avertizează în legătură cu ce vor să publice. Oficialii din domeniul securităţii naţionale le spun apoi redactorilor cum ar putea fi afectată de dezvăluiri securitatea naţională. Are loc o negociere prelungită despre ce se va publica și ce nu. În cel mai bun caz, apare o întârziere substanţială. De cele mai multe ori, informaţia valoroasă este suprimată. Acest lucru a determinat *The Post*, când a relatat despre existenţa închisorilor secrete ale CIA în 2005, să ascundă identităţile ţărilor în care s-au aflat aceste închisori, permiţând ca aceste locuri de tortură ilegale ale CIA să continue să existe.

Același procedeu a determinat *New York Times* să ascundă existenţa[4] programului NSA de supraveghere fără mandat *mai mult de un an* de la momentul în care reporterii săi, James Risen și Eric Lichtblau, erau pregătiţi să-l dezvăluie la jumătatea lui 2004. Președintele Bush i-a convocat pe editorul ziarului, Arthur Sulzberger, și pe redactorul-șef, Bill Keller, în Biroul Oval pentru a insista, în mod ridicol, că ar ajuta teroriștii dacă ar dezvălui că NSA spionează americanii fără mandatele cerute de lege. *New York Times* s-a supus acestor dictate și a blocat publicarea articolului timp de *15 luni* – până la sfârșitul lui 2005, după ce Bush a fost reales (permiţându-i astfel să candideze a doua oară, ascunzând publicului că îi supraveghease pe americani fără mandat). Chiar și atunci, *The Times* a publicat subiectul doar pentru că Risen, frustrat, voia să publice dezvăluirile în cartea sa[5] și ziarul nu voia să i se fure știrea de către propriul reporter.

Apoi, este tonul pe care mass-media apropiată aparatului de stat îl folosește pentru a discuta neregulile guvernamentale. Cultura jurnalismului american împuternicește reporterii să evite orice afirmaţie clară sau declarativă și să încorporeze

aserţiunile administraţiei în relatarea lor, tratându-le cu respect indiferent cât de frivole sunt acestea. Folosesc ceea ce propriul editorialist al *The Post*, Erik Wemple, ridiculizează ca fiind *calea de mijloc*: să nu spui niciodată nimic definitiv, ci să investești cu încredere egală poziția administraţiei și faptele concrete, atenuând astfel efectul dezvăluirilor până la o dezordine confuză, incoerentă și inconsecventă. Mai presus de orice, ei oferă o greutate invariabilă afirmaţiilor oficiale, chiar și când acestea sunt în mod evident false sau înșelătoare.

Jurnalismul dominat de teamă, servil, care a determinat *The Times*, *The Post* și multe alte mijloace de informare în masă să refuze utilizarea cuvântului „tortură“ în relatările lor despre tehnicile de interogare ale administraţiei Bush, chiar și atunci când au folosit în mod liber acest cuvânt pentru a descrie exact aceleași tactici utilizate de alte guverne din lume. Aceasta a produs, de asemenea, potopul mass-media care a spălat afirmaţiile guvernamentale fără fundament despre Saddam și Irak, pentru a vinde publicului american un război construit pe pretexte false, pe care presa americană mai degrabă le-a amplificat decât le-a investigat.

O altă regulă nescrisă desemnată să protejeze administraţia este că aceste organizații media publică doar câteva dintre documentele secrete și apoi se opresc. Ele ar relata despre o arhivă ca a lui Snowden în așa fel încât să îi limiteze impactul – publicând câteva articole, bucurându-se de onorurile unui „subiect exclusiv“, strângând premiile și apoi plecând, asigurându-se că nimic nu s-a schimbat de fapt. Snowden, Laura și cu mine am fost de acord ca, în prezentarea documentelor NSA, să publicăm agresiv, articol după articol, și să nu ne oprim decât atunci când toate subiectele de interes public vor fi acoperite, indiferent câtă furie vor cauza sau câte ameninţări vor provoca ele.

Snowden a fost explicit de la prima noastră conversaţie în legătură cu motivul pentru care nu are încredere în a oferi mass-media apropiate aparatului de stat acest subiect,

referindu-se în mod repetat la ascunderea de către *New York Times* a supravegherii NSA. El a ajuns să creadă că, ascunzând această informaţie, cotidianul a schimbat rezultatul alegerilor din 2004. „Ascunderea acestui subiect a schimbat istoria", a spus el.

Snowden era hotărât să dea în vileag spionajul extrem al NSA dezvăluit de documente, astfel încât aceasta să permită o dezbatere publică de durată și cu consecinţe reale, mai degrabă decât să permită un singur subiect exclusiv care să nu aducă nimic altceva decât distincţii pentru reporteri. Aceasta însemna dezvăluiri curajoase, ignorarea scuzelor șubrede ale administraţiei sau a alarmismului, apărarea fermă a corectitudinii acţiunilor lui Snowden și condamnarea fără echivoc a NSA – exact ceea ce *The Post* ar împiedica reporterii săi să facă atunci când vorbesc despre administraţie. Știam că, orice ar face, *The Post* ar atenua impactul dezvăluirii. Faptul că primiseră o parte din documentele lui Snowden părea total contrar a tot ceea ce eu credeam că încercăm să obţinem.

Ca de obicei, Laura avea motive convingătoare pentru dorinţa ei de a atrage în această poveste *The Post*. Pentru început, ea credea că ar fi benefic ca Washingtonul să fie implicat oficial în dezvăluiri, pentru a le face mai greu de atacat sau incriminat. Dacă ziarul favorit al Washingtonului relata despre subiect, ar fi fost mult mai greu pentru administraţie să îi demonizeze pe cei implicaţi.

Mai mult, așa cum sublinia în mod corect Laura, nici ea și nici Snowden nu putuseră să comunice cu mine uneori din cauza faptului că nu foloseam programe de criptare, și ea fusese cea care purtase povara iniţială de a avea mii de documente strict secrete ale NSA furnizate de sursă. Simţise nevoia de a găsi pe cineva căruia să-i încredinţeze acest material secret și care să lucreze cu o instituţie care să-i ofere o oarecare protecţie. De asemenea, nu voia să călătorească singură către Hong Kong. De vreme ce nu putuse să vorbească cu mine la început, și cât timp sursa simţea că altcineva ar trebui să relateze

despre subiectul PRISM, ea a conchis că e firesc să îl implice pe Gellman.

Am înţeles, dar nu am fost niciodată de acord cu motivele pentru care Laura a vorbit cu *The Post*. Ideea că avem nevoie de implicarea oficială a Washingtonului în subiect era, pentru mine, exact tipul de reticenţă excesivă faţă de asumarea riscurilor și acceptarea regulilor nescrise pe care voiam să-l evit. Eram la fel de buni jurnaliști ca oricine de la *The Post* și, dându-le lor documente pentru a fi protejaţi, susţinea, în viziunea mea, fiecare premisă pe care încercam să o destructurăm. Deși Gellman a sfârșit prin a face o relatare excelentă și importantă pe baza acestor materiale, Snowden, în timpul conversaţiei noastre iniţiale, a început să regrete implicarea *The Post*, chiar dacă el decisese în cele din urmă să accepte recomandarea Laurei de a-i implica.

Snowden era supărat pentru ceea ce percepuse ca fiind tergiversarea *The Post*, prin nechibzuinţa de a implica atât de multe persoane în conversații nesecurizate despre ce a făcut el și, în special, pentru teama demonstrată prin convocarea nesfârșită a avocaţilor alarmiști. Snowden era deosebit de furios că Gellman, la solicitarea avocaţilor și editorilor *The Post,* refuzase în cele din urmă să meargă la Hong Kong pentru a se întâlni cu el și a examina documentele.

Conform lui Snowden și Laurei, avocaţii *The Post* i-au spus lui Gellman că nu ar trebui să meargă la Hong Kong; ei au sfătuit-o și pe Laura să nu meargă și au retras oferta de a-i plăti cheltuielile implicate de călătorie. Aceasta se baza pe o teorie absurdă și generată de teamă că orice discuţie despre informaţii strict secrete desfășurată în China, ea însăși un stat cu supraveghere generalizată, ar putea fi interceptată de guvernul chinez. Acest lucru ar putea fi văzut de administraţia SUA drept o nesăbuinţă din partea *The Post*, care ar transmite în acest fel informaţii secrete Chinei, ceea ce ar putea duce la o responsabilitate penală pentru *The Post* și pentru Gellman în conformitate cu legile privind spionajul.

Snowden, în modul lui stoic și subtil, era foarte furios. Își distrusese viaţa și pusese totul în pericol pentru a scoate la iveală acest subiect. El aproape că nu avea nici un fel de protecţie, iar această organizaţie media uriașă, cu toate tipurile de sprijin legal și instituţional, nu își asuma riscul banal de a trimite un reporter la Hong Kong pentru a se întâlni cu el. „Sunt dispus să le ofer acest subiect uriaș în ciuda riscului personal imens", a spus el, „iar ei nici măcar nu se urcă într-un avion." Era exact tipul de obedienţă guvernamentală timidă și refractară la riscuri pe care am petrecut ani la rând condamnând-o.

Faptul de a oferi unele dintre documente cotidianului *The Post* era consumat și nu puteam face nimic nici eu, nici el în legătură cu acest lucru. Dar în a doua noapte petrecută în Hong Kong, după ce m-am întâlnit cu Snowden, am hotărât că nu *Washington Post*, cu vocea sa proguvernamentală, confuză, cu teama sa și calea sa de mijloc, va fi cel care va modela felul în care vor fi înţeleși pentru totdeauna NSA și Snowden. Oricine va scrie primul despre acest subiect va juca un rol predominant în modul în care acesta va fi discutat și încadrat, și era hotărât ca primele articole să fie scrise de *Guardian* și de mine. Pentru ca acest subiect să aibă efect, regulile nescrise ale jurnalismului apropiat puterii – desemnat să atenueze impactul dezvăluirilor și să protejeze administraţia – trebuiau încălcate, nu respectate. *The Post* le-ar respecta – eu nu.

Așadar, ajuns în camera mea de hotel, am terminat de scris cele patru articole. Primul era despre ordinul secret din partea tribunalului FISA, care obliga Verizon, una dintre cele mai mari companii de telefonie americane, să preda NSA toate înregistrările telefonice ale tuturor americanilor. Al doilea acoperea subiectul programului de spionare fără mandat al lui Bush, bazat pe un raport intern strict secret din 2009 din partea inspectorului general al NSA; altul detalia programul BOUNDLESS INFORMANT, despre care citisem în avion; ultimul articol descria programul PRISM, despre care aflasem pentru prima dată în timp ce eram acasă, în Brazilia. Acest

subiect, înainte de toate, mă obliga să mă mișc repede: era documentul la care lucra *The Post*.

În consecință, aveam nevoie ca *Guardian* să publice imediat. În timp ce la Hong Kong se apropia seara – iar la New York era dimineaţa devreme –, așteptam cu nerăbdare ca editorii *Guardian* să se trezească la New York și verificam la fiecare cinci minute să văd dacă Janine Gibson a intrat pe chatul Google, modul nostru de a comunica. Imediat ce am văzut-o online, i-am trimis un mesaj: „Trebuie să vorbim".

Știam deja că vorbitul la telefon sau prin chatul Google ieșeau din discuţie. Amândouă modalităţile erau mult prea nesigure. Nu am reușit, din nu știu ce motive, să ne conectăm prin OTR, programul de comunicare criptat pe care îl foloseam, așa că Janine a sugerat să încercăm Cryptocat, un program recent, conceput să împiedice supravegherea din partea statului, care a devenit principalul nostru mod de comunicare în perioada pe care eu am petrecut-o la Hong Kong.

I-am spus despre întâlnirea mea din ziua respectivă cu Snowden, că eram convins de autenticitatea lui și a documentelor pe care le furnizase. I-am spus că am scris deja câteva articole. Janine era deosebit de entuziasmată de povestea cu Verizon.

„Grozav", am spus. „Articolul ăsta este gata. Dacă mai sunt corecturi minore, bine, haide să le facem". I-am subliniat lui Janine necesitatea publicării rapide. „Haide să-i dăm drumul acum."

Dar era o problemă. Redactorii *Guardian* se întâlniseră cu avocaţii ziarului și fuseseră puși în faţa unor avertizări alarmante. Janine mi-a transmis ceea ce îi spuseseră avocaţii *Guardian*: publicarea unor informaţii secretizate poate fi descrisă (chiar dacă discutabil) drept o infracţiune de către administraţia americană, o încălcare a Legii Spionajului, chiar și pentru ziare. Pericolul era deosebit de mare în ceea ce privește documentele ce aveau legătură cu serviciile secrete. Administraţia se abţinuse să pună sub acuzare mass-media în trecut,

dar doar atât timp cât presa respecta reguli nescrise în conformitate cu care le oferea oficialilor posibilitatea de a citi materialul înainte de publicare și de a argumenta că publicarea lui va periclita securitatea naţională. Acest proces consultativ cu administraţia, au explicat avocaţii *Guardian*, este ceea ce le permite ziarelor să demonstreze că nu au nici o intenţie de a prejudicia securitatea naţională publicând documente strict secrete. În același timp, se asigurau astfel că nu vor fi urmăriți în justiţie.

Niciodată nu existase o scurgere de documente de la NSA, fără a mai pune la socoteală una cu o astfel de amploare și atât de sensibilă. Avocaţii credeau că există o potenţială expunere penală – nu numai pentru Snowden, ci, având în vedere istoricul administraţiei Obama, și pentru ziar. Cu doar câteva săptămâni înainte de sosirea mea la Hong Kong se dezvăluise că Departamentul de Justiţie din administraţia Obama obţinuse o hotărâre judecătorească să citească e-mailurile și înregistrările telefonice ale reporterilor și redactorilor Associated Press[6] pentru a afla sursa unui subiect.

Aproape imediat după aceasta, o altă relatare a dezvăluit un atac și mai extrem asupra procesului de strângere de informaţii: Departamentul de Justiţie depusese la tribunal un afidavit prin care îl acuza pe șeful biroului din Washington al Fox News, James Rosen[7], că este un „participant" la presupusele infracţiuni comise de sursa lui, pe motivul că jurnalistul a „ajutat și instigat" sursa să dezvăluie informaţii secretizate, colaborând cu aceasta îndeaproape pentru a primi materiale.

Jurnaliștii remarcaseră de câţiva ani că administraţia Obama desfășoară atacuri fără precedent la adresa jurnalismului. Dar episodul Rosen a întrecut orice limită. Să incriminezi cooperarea cu sursa ca „ajutor și instigare" înseamnă să incriminezi jurnalismul de investigaţie în sine: nici un reporter nu obţine informaţii secrete fără să colaboreze cu sursa lui pentru a ajunge la ele. Acest climat determinase pe toţi avocaţii

organizaţiilor de presă, inclusiv pe cei ai *Guardian*, să fie extrem de precauţi și chiar temători.

„Ei spun că FBI ar putea veni și închide biroul și ar putea să ne ia dosarele“, mi-a spus Gibson.

M-am gândit că este ridicol: însăși ideea că administraţia SUA ar putea închide un ziar mare ca *Guardian US* și efectua raiduri în birourile acestuia era tipul de sfat extrem de îngrijorător care m-a făcut, în cariera mea juridică, să învăţ să urăsc avertizările excesive și inutile ale avocaţilor. Dar știam că Gibson nu ar fi respins și nu ar fi putut să respingă, pur și simplu și fără ezitare, aceste îngrijorări.

„Ce implică acest lucru în ceea ce ne privește?“, am întrebat. „Când putem publica?“

„Nu sunt sigură, Glenn“, mi-a spus Gibson. „Mai întâi trebuie să sortăm totul. Ne întâlnim cu avocaţii din nou mâine și vom ști mai multe atunci.“

Eram cu adevărat îngrijorat. Nu aveam nici o idee cum vor reacţiona redactorii *Guardian*. Independenţa mea la *Guardian* și faptul că scrisesem puţine articole cu o consultare editorială și cu siguranţă nu atât de sensibile ca acesta mă îndreptățeau să cred că am de-a face cu factori necunoscuţi. Într-adevăr, întreaga poveste era de o noutate absolută: era imposibil să știu cum va reacţiona cineva, pentru că nu se mai întâmplase ceva similar înainte. Se vor lăsa redactorii speriaţi și intimidaţi de ameninţările guvernului? Vor opta să petreacă săptămâni întregi în negocieri cu administraţia? Vor prefera să lase *The Post* să dea știrea primul, ca să se simtă mai în siguranţă?

Eram nerăbdător să public povestea cu Verizon imediat: aveam documentul FISA și era clar adevărat. Nu exista nici un motiv pentru a le refuza americanilor dreptul de a vedea ce face administraţia cu viaţa lor privată, nici măcar un minut. La fel de presantă era obligaţia pe care o simţeam faţă de Snowden. El făcuse alegerea în spiritul curajului, al pasiunii și al convingerii. Eram hotărât ca tot ce scriam să fie în același spirit, de a face dreptate pentru sacrificiul pe care

sursa noastră îl făcuse. Doar jurnalismul îndrăzneţ poate da subiectului puterea de care are nevoie pentru a depăși teama pe care administrația o impusese jurnaliștilor și surselor lor. Avertizările legale paranoice și ezitarea *Guardian* erau antiteza unei astfel de îndrăzneli.

În acea noapte l-am sunat pe David și i-am mărturisit îngrijorarea mea tot mai mare în legătură cu *Guardian*. Am discutat despre aceste îngrijorări și cu Laura. Am fost de acord să lăsăm timp ziarului *Guardian* până a doua zi pentru a publica primul articol, după care urma să explorăm alte opţiuni.

După câteva ore, Ewen MacAskill a venit în camera mea ca să primească date actualizate despre Snowden, pe care încă nu îl întâlnise. Am împărtășit cu el îngrijorările mele în legătură cu întârzierile. „Nu trebuie să îţi faci griji", a spus el despre *Guardian*. „Sunt foarte agresivi." Alan Rusbridger, redactorul-șef din Londra al *Guardian*, este „foarte implicat" în subiect și „decis să publice", m-a asigurat el.

Încă îl vedeam pe Ewen ca pe reprezentantul companiei, dar atitudinea mea se îmbunătăţea ușor în ceea ce îl privește, având în vedere dorinţa lui de a publica rapid. După ce a plecat, i-am spus lui Snowden că Ewen a călătorit cu noi, numindu-l „babysitter"-ul *Guardian*, și i-am spus că vreau să se întâlnească cu el a doua zi. I-am explicat că faptul că l-am luat cu noi pe Ewen a fost un pas important în a-i face pe redactorii *Guardian* să se simtă suficient de confortabil pentru a publica. „Nici o problemă", a spus Snowden. „Dar știi că ai un om de pază. De aceea l-au trimis."

Întâlnirea lor era importantă. În dimineaţa următoare, Ewen a venit cu noi la hotelul lui Snowden și am petrecut două ore dure chestionându-l, acoperind în mare parte același teren ca în ziua precedentă. „Cum pot ști că ești ceea ce spui că ești?", a întrebat Ewen la final. „Ai vreo dovadă?" Snowden a scos din geantă un vraf de documente: pașaportul său diplomatic expirat, un fost card de identificare CIA, un permis de conducere și un alt act de identitate guvernamental.

Am plecat de la hotel împreună. „Sunt convins în totalitate că este real“, a spus Ewen. „Nu am nici o îndoială.“ În opinia sa, nu mai era nici un motiv să așteptăm. „Îl voi suna pe Alan imediat ce vom ajunge la hotel și îi vom spune că ar trebui să înceapă să publice acum.“

Din acel moment, Ewen a fost integrat total în echipa noastră. Laura și Snowden s-au simţit imediat confortabil în prezenţa lui, iar eu a trebuit să mărturisesc că simțeam același lucru. Mi-am dat seama că suspiciunile noastre erau total nefondate: dincolo de aspectul exterior manierat și prietenos, Ewen era un reporter curajos, dornic să prezinte acest subiect exact așa cum credeam cu toţii că este necesar. Ewen, cel puţin așa cum se vedea el, nu era acolo pentru a impune constrângeri instituţionale, ci pentru a relata și, uneori, pentru a ajuta la depășirea acelor constrângeri. De fapt, pe durata șederii noastre în Hong Kong, Ewen a fost de multe ori vocea cea mai radicală, argumentând în favoarea dezvăluirilor pe care nici chiar eu sau Laura – or, la drept vorbind, nici Snowden – nu eram siguri că ar trebui făcute. Ne-am dat seama rapid că faptul că milita pentru o relatare agresivă în cadrul *Guardian* va fi vital în a păstra Londra implicată în ce făceam, și așa a fost.

Imediat ce s-a făcut dimineaţă la Londra, împreună cu Ewen l-am sunat pe Alan. Voiam să transmit cât mai clar posibil că am așteptat – am cerut chiar – ca *Guardian* să înceapă publicarea în acea zi și să aflu poziţia clară a ziarului. La acel moment – doar a doua mea zi plină în Hong Kong – eram pregătit mental să duc subiectul în altă parte dacă simţeam o ezitare instituţională substanţială.

Am fost sincer. „Sunt pregătit să public articolul despre Verizon și nu înţeleg deloc de ce nu o facem acum“, i-am spus lui Alan. „De ce această întârziere?“

El m-a asigurat că nu este nici o întârziere. „Sunt de acord. Suntem gata să publicăm. Janine urmează să aibă o ultimă întâlnire cu avocaţii în această după-amiază. Sunt sigur că vom publica după aceasta.“

Am adus în discuţie implicarea *The Post* în subiectul PRISM, care nu făcea decât să alimenteze sentimentul meu că lucrurile sunt urgente. Atunci Alan m-a luat prin surprindere: nu numai că voia să fie primul care publică articolele despre NSA în general, dar voia să fie primul care publică articolul despre PRISM în mod particular, în mod clar dornic să ia exclusivitatea de la *Post*. „Nu există nici un motiv pentru care să le-o cedăm", a spus el.

„Sunt perfect de acord."

Londra este cu patru ore înaintea New Yorkului, așa că mai dura ceva până când Janine mergea la birou și chiar și mai mult până când se întâlnea cu avocaţii. Prin urmare am petrecut seara la Hong Kong cu Ewen, finalizând articolul despre PRISM, convins că Rusbridger va fi atât de agresiv cât va fi nevoie.

Am terminat articolul despre PRISM în ziua respectivă și am folosit programul de criptare pentru a-l trimite prin e-mail lui Janine și lui Stuart Millar, la New York. Acum aveam două subiecte exclusive majore gata de publicare: Verizon și PRISM. Răbdarea mea, dorinţa mea de a aștepta se epuizau rapid.

Janine și-a început întâlnirea cu avocaţii la 15.00, ora New Yorkului – 03.00, ora Hong Kongului – și a stat cu ei două ore. Am stat treaz, așteptând să aflu rezultatul. Când am vorbit cu Janine, voiam să aud un singur lucru: că îi dăm drumul imediat articolului despre Verizon.

Nu s-a întâmplat așa, nici pe departe. Încă erau probleme legale „considerabile" de rezolvat, mi-a spus ea. Odată ce acestea vor fi rezolvate, *Guardian* va trebui să avertizeze oficialii guvernamentali în legătură cu planurile noastre, pentru a le oferi oportunitatea să ne convingă să nu publicăm – proces pe care îl detestam și îl condamnasem îndelung. Am acceptat că *Guardian* va trebui să lase administraţia să-și expună argumentele împotriva publicării, cu condiţia ca procesul să nu devină un mijloc prelungit de amânare a subiectului timp de mai multe săptămâni, pentru a-i atenua impactul.

„Sună de parcă suntem la zile sau chiar săptămâni de publicare, nu ore“, i-am spus lui Janine, încercând să transmit toată iritarea și nerăbdarea mea în discuţia online. „Dă-mi voie să-ţi repet că voi lua orice măsură necesară pentru a mă asigura că această poveste vede tiparul acum.“ Ameninţarea era implicită, dar clară: dacă nu văd articolele imediat în *Guardian*, voi merge în altă parte.

„Ai fost deja foarte clar în această privinţă“, a replicat ea tăios.

Era seară la New York și știam că nu se va întâmpla nimic până a doua zi. Eram frustrat și, din acest motiv, foarte anxios. *The Post* lucra la articolul despre PRISM, iar Laura, care urma să fie trecută drept unul dintre autori, a auzit de la Gellman că plănuiau să publice duminică, ceea ce însemna peste cinci zile.

Vorbind despre acest lucru cu David și Laura, mi-am dat seama că nu mai voiam să aștept *Guardian*. Am fost cu toţii de acord că ar trebui să explorăm alternativa pentru un Plan B, în eventualitatea în care va apărea o întârziere mai mare. Apeluri telefonice la *Salon*, unde publicam de ani întregi, precum și la *Nation*, au dat roade rapid. Amândouă mi-au spus în decurs de câteva ore că ar fi bucuroase să publice articolele despre NSA imediat și mi-au oferit tot sprijinul de care aș avea nevoie, cu avocaţi dispuși să verifice articolele imediat.

Faptul că știam că sunt două locuri consacrate dispuse și dornice să publice articolele despre NSA era încurajator. Dar în conversaţiile cu David, am decis că exista o alternativă și mai puternică: să creăm pur și simplu propriul nostru website, intitulat NSAdisclosures.com, și să începem să difuzăm articolele acolo, fără să mai fie nevoie de vreo organizaţie de presă existentă. Odată ce vom face public că deţinem această comoară imensă de documente secrete despre spionajul efectuat de NSA, vom recruta cu ușurinţă redactori voluntari, avocaţi, cercetători și susţinători financiari – o întreagă echipă, motivată de nimic altceva decât de entuziasmul pentru transparenţă și un jurnalism combativ real, devotat relatării a ceea ce

știam că este cea mai semnificativă scurgere de informaţii din istoria SUA.

De la început, am crezut că documentele prezentau o oportunitate de a scoate la lumină nu numai spionajul secret al NSA, ci și caracterul corupt al dinamicii jurnalismului consacrat. Să public unul dintre cele mai importante subiecte de-a lungul anilor într-o formă nouă și independentă de relatare, separat de orice organizaţie de presă importantă, era extrem de atrăgător pentru mine. Voi sublinia cu îndrăzneală că garanţia oferită de Primul Amendament pentru o presă liberă și capacitatea de a face jurnalism de valoare nu depind de afilierea la o organizaţie mass-media consacrată. Garanţia presei libere nu protejează doar reporterii care fac parte din corporaţii, ci pe oricine este implicat în jurnalism, fie că este angajat sau nu. Și curajul transmis în acest fel – *Vom publica mii de documente strict secrete ale NSA fără protecţia unei corporaţii media importante* – îi va încuraja și pe alţii și va contribui la distrugerea actualului climat de teamă.

În acea noapte abia dacă am dormit. Am petrecut primele ore ale dimineţii în Hong Kong sunând persoane în ale căror opinii am încredere: prieteni, avocaţi, jurnaliști, persoane cu care am lucrat îndeaproape. Toate mi-au dat același sfat: este prea riscant să fac acest lucru singur, fără o structură media existentă. Voiam să aud argumente împotriva unei acţiuni independente și ei mi-au oferit multe și bune.

Mai târziu în aceeași dimineaţă, după ce am auzit toate avertizările, l-am sunat din nou pe David, în timp ce vorbeam online cu Laura. David era ferm că recurgerea la *Salon* sau *Nation* ar fi fost un gest care transmitea prea multă precauţie și teamă – „un pas înapoi“, cum i-a spus el – și astfel, în cazul în care *Guardian* amâna în continuare, doar publicarea articolelor pe un website nou creat putea capta spiritul cutezător care conducea acest demers. El era, de asemenea, convins că acest lucru ar fi fost un model de inspiraţie pentru persoanele din întreaga lume. Deși iniţial sceptică, Laura era convinsă că un

astfel de pas îndrăzneţ – crearea unei reţele de persoane dedicate transparenţei NSA – ar dezlănţui un val masiv și puternic de entuziasm.

Așadar, cum la Hong Kong se apropia după-amiaza, am decis de comun acord că, dacă *Guardian* nu vrea să publice până la sfârșitul zilei respective – care încă nu începuse pe Coasta de Est –, voi pleca și voi posta imediat articolul despre Verizon pe noul nostru website. Deși înţelesesem riscurile implicate, eram incredibil de entuziasmat de decizia noastră. Știam și că având acest plan alternativ deveneam mai puternic în discuţia din ziua respectivă cu *Guardian*; simţeam că nu mai trebuie să rămân legat de ei pentru relatarea acestui subiect, iar eliberarea de atașamente te face întotdeauna mai puternic.

Când am vorbit cu Snowden în acea după-amiază, i-am spus despre planul nostru. „Riscant. Dar îndrăzneţ“, a scris el. „Îmi place.“

Am reușit să dorm câteva ore, m-am trezit în mijlocul după-amiezii la Hong Kong și apoi m-am confruntat cu faptul că aveam de așteptat ore întregi până se va face miercuri dimineaţă la New York. Știam că, într-un fel, voi comunica un ultimatum ziarului *Guardian*. Voiam să trec direct la acest lucru.

Imediat ce am văzut că Janine a intrat online, am întrebat-o care este planul. „Veţi publica astăzi?“

„Sper“, a răspuns ea. Nesiguranţa ei m-a agitat. *Guardian* încă intenţiona să contacteze NSA în acea dimineaţă pentru a-i avertiza în legătură cu intenţiile noastre. A spus că vom ști programul de publicare doar după ce ne vor răspunde.

„Nu pricep de ce trebuie să așteptăm“, am spus, pierzându-mi răbdarea în faţa amânărilor din partea *Guardian*. „Pentru un articol atât de curat și direct, cui îi pasă ce cred ei că ar trebui să publicăm sau nu?“

În afară de dispreţul meu faţă de proces – administraţia nu ar trebui să fie un partener editorial care să colaboreze cu un ziar în decizia acestuia cu privire la ce să fie publicat –, știam

că nu există un argument plauzibil cu privire la securitatea naţională împotriva articolului nostru despre Verizon, care implica doar un ordin judecătoresc ce arăta colectarea sistematică a datelor telefonice ale americanilor. Ideea că „teroriștii" ar beneficia de dezvăluirea acestui ordin ar fi fost derizorie: orice terorist capabil să se lege singur la șireturi știe că administraţia încearcă să îi monitorizeze comunicaţiile telefonice. Persoanele care ar afla ceva din articolul nostru nu ar fi „teroriștii", ci poporul american.

Janine a repetat ce aflase de la avocaţii *Guardian* și a insistat că plec de la presupunerea greșită că mă gândesc că ziarul se va lăsa intimidat și nu va publica. În schimb, a spus ea, este o cerinţă legală ca ei să asculte ce au de spus oficialii americani. Dar, m-a asigurat ea, nu va fi intimidată sau controlată de apelurile vagi și frivole la securitatea naţională.

Nu am presupus că *Guardian* va fi intimidat; pur și simplu nu știam. Și eram îngrijorat că, în cele din urmă, discuţia cu administraţia va întârzia lucrurile prea mult. *Guardian* avea reputația că relatează agresiv și sfidător – unul dintre motivele pentru care am mers acolo în primul rând. Și știam că aveau dreptul să demonstreze ce ar face în această situaţie înainte ca eu să presupun ce este mai rău. Proclamaţia de independenţă a lui Janine a fost cumva liniștitoare.

„OK", am spus, dispus să aștept și să văd. „Dar, încă o dată, din perspectiva mea, materialele ar trebui publicate *astăzi*", am scris. „Nu sunt dispus să mai aștept."

În jurul prânzului la New York, Janine mi-a spus că au sunat la NSA și la Casa Albă ca să le spună că intenţionează să publice materiale strict secrete. Nimeni nu i-a sunat înapoi. Casa Albă o numise în acea dimineaţă pe Susan Rice în funcţia de consilier pentru securitatea naţională. Reporterul *Guardian* pentru securitate naţională, Spencer Ackerman, avea contacte bune la Washington. El i-a spus lui Janine că oficialii sunt „ocupaţi" cu Susan Rice.

„În acest moment, ei nu cred că trebuie să ne sune înapoi“, a scris Janine. „Vor afla rapid că trebuie să răspundă la telefoanele mele.“

La ora 03.00 – 15.00 la New York – încă nu aveam nici o veste. Și nici Janine.

„Au vreun termen limită sau ne răspund când vor ei?“, am întrebat sarcastic.

Ea mi-a răspuns că *Guardian* a cerut să i se răspundă din partea NSA „până la sfârșitul zilei“.

„Și dacă nu răspund până atunci?“, am întrebat.

„Ei bine, vom lua o decizie la momentul respectiv“, a spus ea.

Janine a adăugat apoi un alt factor care complica lucrurile: Alan Rusbridger, șeful ei, tocmai urcase într-un avion de la Londra la New York, să supravegheze publicarea articolelor despre NSA. Dar aceasta însemna că va fi imposibil de contactat în următoarele șapte ore sau undeva pe acolo.

„Poţi să publici acest articol fără Alan?“. Dacă răspunsul era „nu“, atunci nu exista nici o șansă ca articolul să fie publicat în ziua respectivă. Avionul lui Alan nici măcar nu era programat să ajungă pe aeroportul JFK până târziu în noapte.

„Vom vedea“, a spus ea.

Am simţit că mă lovesc de exact aceleași bariere instituţionale de a relata agresiv pentru a căror evitare m-am alăturat *Guardian*: îngrijorările juridice. Consultarea cu oficialii guvernamentali. Ierarhiile instituţionale. Aversiunea faţă de risc. Amânarea.

După câteva momente, la aproximativ 15.15 ora New Yorkului, Stuart Millar, adjunctul lui Janine, mi-a trimis un mesaj: „Administraţia a sunat înapoi. Janine vorbește cu ei acum“.

Am avut senzația că am așteptat o eternitate. După aproximativ o oră, Janine m-a sunat și mi-a povestit ce s-a întâmplat. Au fost aproape 12 oficiali de rang înalt la telefon de la numeroase agenţii, inclusiv NSA, DOJ [Departamentul de Justiţie] și Casa Albă. La început au fost respectuoși, dar

amabili, spunându-i că nu înţeleg semnificaţia sau „contextul“ ordinului judecătoresc privind Verizon. Voiau să programeze o întâlnire cu ea „cândva săptămâna următoare“ pentru a explica lucrurile.

Când Janine le-a spus că vrea să publice în ziua respectivă și că va face acest lucru dacă nu primește un motiv clar și concret care să o împiedice, au devenit mai combativi, chiar amenințători. I-au spus că nu este o „jurnalistă serioasă“ și că *Guardian* nu este un „ziar serios“, pentru că refuză să acorde administraţiei mai mult timp pentru a argumenta în favoarea renunțării la articol.

„Nici un ziar normal nu ar publica acest lucru imediat, fără să se întâlnească mai întâi cu noi“, au spus ei, pledând clar în favoarea obţinerii unei amânări.

Probabil că au dreptate, îmi aduc aminte că m-am gândit. Aceasta este și ideea. Regulile în vigoare permit administraţiei să controleze și să neutralizeze procesul de strângere de informaţii și să elimine relaţia antagonică dintre presă și administraţie. Pentru mine era vital ca ei să știe de la început că aceste reguli neprincipiale nu vor fi aplicate în cazul nostru. Aceste articole vor fi publicate sub un set de reguli diferit, unul care va defini mai degrabă un corp de presă independent, decât servil. Eram încurajat de tonul lui Janine: puternic și sfidător. Ea a subliniat că, în pofida solicitării ei repetate, ei nu au reușit să ofere nici un singur argument în favoarea faptului că securitatea naţională ar fi prejudiciată de această publicare. Dar încă nu promisese că va publica în ziua respectivă. La încheierea convorbirii, a spus: „O să văd dacă îl pot contacta pe Alan, apoi vom decide ce vom face“.

Am așteptat jumătate de oră, apoi am întrebat-o răspicat: „Vei publica astăzi sau nu? Asta e tot ce vreau să știu“.

A evitat întrebarea. Alan era imposibil de contactat. Era clar că ea se află într-o situaţie extrem de dificilă: pe de o parte, oficialii americani o acuzau vehement de necugetare; pe de altă parte, mă avea pe mine făcând solicitări tot mai departe

de compromis. Și, mai presus de toate, redactorul-șef al ziarului era într-un avion, ceea ce făcea ca una dintre cele mai dificile și mai pline de consecințe decizii din istoria de 190 de ani a ziarului să cadă direct pe umerii ei.

În timp ce vorbeam online cu Janine, eram la telefon cu David. „Este aproape ora 17.00“, a afirmat David. „Acesta este termenul limită pe care l-ai dat. E timpul pentru o decizie. Trebuie să publice acum sau trebuie să le spui că duci materialele în altă parte.“

Avea dreptate, dar ezitam. Să plec de la *Guardian* chiar înainte de a publica una dintre cele mai mari scurgeri de informaţii despre securitatea naţională din istoria SUA va provoca un scandal media uriaș. Aș fi discreditat la maximum *Guardian* și ar fi trebuit să ofer o explicaţie publică, fapt care i-ar fi obligat pe ei să se apere, probabil atacându-mă. Ar fi ieșit un circ, un uriaș spectacol colateral care ne-ar fi făcut rău tuturor. Mai mult, ne-ar fi distras atenţia de la subiectul asupra căruia trebuia să ne concentrăm: dezvăluirile privind NSA.

Trebuie să recunosc și teama mea personală: publicarea a sute, dacă nu mii de documente strict secrete ale NSA era suficient de riscantă chiar și pentru o organizaţie mare ca *Guardian*. Să fac acest lucru singur, fără o protecţie instituţională, ar fi fost și mai riscant. Toate avertizările inteligente din partea prietenilor și avocaţilor pe care îi sunasem îmi răsunau puternic în cap.

În timp ce ezitam, David a spus: „Nu ai de ales. Dacă sunt speriaţi să publice, atunci acesta nu este locul potrivit pentru tine. Nu poţi acţiona din teamă pentru că nu obţii nimic. Aceasta este lecţia pe care Snowden tocmai ţi-a servit-o“.

Împreună, am compus ceea ce urma să îi spun lui Janine în discuţia noastră online: „Este ora 17.00, iar acesta a fost termenul limită pe care ţi l-am oferit. Dacă nu publici imediat – în următoarele 30 de minute –, atunci prin prezenta îmi închei contractul cu *Guardian*“. Eram aproape să apăs pe

„trimite“, după care m-am mai gândit. Nota aducea prea mult cu o ameninţare explicită.

Dacă plec de la *Guardian* în aceste circumstanţe, va fi făcut public totul, inclusiv această frază. Așa că am îndulcit tonul: „Înţeleg că ești îngrijorată și că trebuie să faci ceea ce simţi că este corect. Voi merge înainte și voi face acum ceea ce cred eu că trebuie făcut. Îmi pare rău că nu a mers“. După care am apăsat „trimite“.

În 15 secunde, telefonul a sunat în camera mea de hotel. Era Janine. „Cred că ești îngrozitor de nedrept“, a spus ea, în mod evident foarte supărată. Dacă plecam, *Guardian* – care nu avea nici unul dintre documente – ar fi pierdut tot subiectul.

„Cred că tu ești cea nedreaptă“, am replicat. „Te-am întrebat în mod repetat când intenţionezi să publici și ai refuzat să îmi răspunzi, eschivându-te.“

„Vom publica astăzi“, a spus Janine. „În cel mult 30 de minute. Eram la corectura finală, lucram la titluri și formă. Va fi încărcat nu mai târziu de 17.30.“

„OK. Dacă acesta este planul, atunci nu e nici o problemă“, am spus. „Evident că sunt dispus să aștept 30 de minute.“

La 17.40, Janine mi-a trimis un mesaj pe chat cu un link, cel pe care îl așteptam de zile întregi. „Este publicat“, a spus ea.

„NSA strânge zilnic date telefonice de la milioane de clienţi Verizon“, era titlul, urmat de un subtitlu: „Exclusiv: Ordinul judecătoresc strict secret care cere Verizon să predea toate datele telefonice arată amploarea supravegherii interne în cadrul administraţiei Obama“.

După care urma un link către ordinul tribunalului FISA. Primele trei paragrafe ale articolului nostru spuneau toată povestea:

> Agenția pentru Securitate Națională [NSA] colectează în prezent date telefonice de la milioane de clienți americani ai Verizon, unul dintre cei mai mari furnizori de telecomunicații din America, în conformitate cu un ordin judecătoresc strict secret emis în aprilie.

> Ordinul, a cărui copie a fost obținută de *Guardian*, cere Verizon ca „zilnic şi în mod continuu“ să ofere NSA informații despre toate apelurile telefonice din sistemele sale, atât din interiorul SUA, cât şi dintre SUA şi alte țări.
>
> Documentul arată pentru prima dată că în administrația Obama datele comunicațiilor a milioane de cetățeni americani sunt colectate fără discriminare şi în masă – indiferent dacă aceştia sunt sau nu suspectați de vreo infracțiune.

Impactul articolului a fost instantaneu și enorm, dincolo de ce anticipasem. A fost subiectul principal la fiecare jurnal de știri din seara respectivă și a dominat discuţiile politice și mediatice. Am primit nenumărate solicitări de interviu de la aproape toate posturile naţionale de televiziune: CNN, MSNBC, NBC, *Today show, Good Morning America* și altele. Am petrecut multe ore în Hong Kong vorbind cu numeroși moderatori de televiziune agreabili – o experienţă neobișnuită în cariera mea de scriitor politic adeseori în conflict cu presa apropiată aparatului de stat –, care au tratat cu toţii subiectul ca pe un eveniment major și un real scandal.

Ca reacție, purtătorul de cuvânt al Casei Albe a apărat, cum era de așteptat, întregul program de colectare de date, socotindu-l „o unealtă critică pentru protejarea națiunii de amenințările terorismului“. Președinta democrată a Comisiei pentru serviciile de informații din Senat, Dianne Feinstein, unul dintre cei mai înfocați susținători în Congres ai securității naționale și mai ales ai serviciilor de supraveghere americane, a invocat situația de după 11 septembrie spunându-le reporterilor că programul era necesar fiindcă „oamenii voiau ca țara lor să fie pusă la adăpost“.

Dar aproape nimeni nu a luat aceste afirmaţii în serios. Pagina editorială a *New York Times*, pro-Obama, a denunţat aspru administraţia. Într-un editorial intitulat „Plasa de pescuit a președintelui Obama“, ziarul anunţa: „Domnul Obama demonstrează truismul că ramura executivă va folosi orice putere i se dă și foarte probabil va abuza de ea“. Luând în derâdere

invocarea mecanică de către administraţie a „terorismului" pentru a justifica programul, editorialul proclama: „Administraţia și-a pierdut acum toată credibilitatea". (Generând o oarecare controversă, *New York Times*, fără să comenteze, a îndulcit această denunţare severă[8] la câteva ore după prima publicare adăugând sintagma „pe acest subiect").

Senatorul democrat Mark Udall a publicat o declaraţie[9] în care afirma că „astfel de supraveghere la scară largă ar trebui să ne îngrijoreze pe toţi și este tipul de depășire a atribuţiilor de către administraţie despre care am spus că americanii o vor considera șocantă". ACLU a spus că „din perspectiva libertăţilor civile, programul ar putea cu greu să fie mai alarmant...[10] Este mai mult decât orwellian și oferă dovezi în plus despre cât de mult se renunță în secret la drepturile democratice elementare în fața solicitărilor nenumărate ale agenţiilor de informaţii". Fostul vicepreședinte Al Gore a scris pe Twitter, cu link către articolul nostru: „Mi se pare mie sau supravegherea generalizată este nerușinat de scandaloasă?".[11]

Curând după publicarea articolului, Associated Press a obţinut din partea unui senator căruia nu i-a dat numele confirmarea a ceea ce suspectam deja: că programul de colectare masivă a înregistrărilor telefonice a fost activ ani de zile și a fost direcţionat către toţi furnizorii majori de telecomunicaţii din SUA, nu doar Verizon.

În cei șapte ani în care scrisesem și vorbisem despre NSA, nu văzusem niciodată o dezvăluire care să producă ceva similar cu acest nivel de interes și înflăcărare. Nu era timp să analizăm de ce rezonase atât de puternic și generase un astfel de val de interes și indignare; pentru moment, intenţionam să rămân pe val mai degrabă decât să încerc să îl înţeleg.

Când am terminat în cele din urmă cu interviurile TV, aproape de prânz ora Hong Kongului, am mers direct în camera de hotel a lui Snowden. Când am intrat, se uita la CNN. Invitaţii discutau despre NSA, exprimându-și șocul faţă de amploarea programului de spionaj. Gazdele erau indignate

că totul s-a făcut în secret. Aproape fiecare invitat pe care îl aduceau denunţa spionajul intern în masă.

„Este peste tot“, a spus Snowden, în mod clar entuziasmat. „M-am uitat la toate interviurile tale. Toată lumea pare să prezinte știrea.“

La acel moment, am simţit cu adevărat o realizare. Teama majoră a lui Snowden – că dă cu piciorul la viaţa lui pentru dezvăluiri de care nu i-ar păsa nimănui – se dovedise nefondată din acea primă zi: nu am văzut nici o urmă de indiferenţă sau apatie. Laura și cu mine îl ajutaserăm să declanșeze dezbaterea despre care toţi credeam că este necesară în mod urgent – iar acum îl puteam vedea cum urmărește desfășurarea ei.

Având în vedere planul lui Snowden de a se deconspira după prima săptămână de articole, știam amândoi că libertatea lui se apropia foarte repede de sfârșit. Pentru mine, siguranţa deprimantă că va deveni în curând ţinta atacurilor – vânat, dacă nu închis ca un infractor – plana peste tot ceea ce făcuserăm. Pe el nu părea să îl deranjeze deloc, dar m-a făcut pe mine mai hotărât să îi apăr alegerea, să maximizez valoarea dezvăluirilor pentru care riscase totul. Ne aflam în faţa unui start bun și era doar începutul.

„Toată lumea crede că este vorba despre un singur articol, un subiect exclusiv izolat“, a remarcat Snowden. „Nimeni nu știe că este doar vârful aisbergului, că urmează mult mai mult“. S-a întors către mine. „Ce urmează și când?“

„PRISM“, am spus. „Mâine.“

M-am întors la hotelul meu și, în pofida faptului că mă apropiam de cea de-a șasea noapte nedormită, pur și simplu nu puteam închide ochii. Adrenalina era mult prea puternică. La ora 16.30, când era singura mea speranţă să prind un pic de somn, am luat o pastilă și am setat alarma la 19.30, când știam că redactorii *Guardian* din New York vor intra online.

În ziua aceea, Janine a intrat online devreme. Ne-am felicitat și ne-am mirat de reacţia la articol. Imediat a fost evident

că tonul discuției noastre se schimbase radical. Traversaserăm împreună o provocare jurnalistică semnificativă. Janine era mândră de articol și eu eram mândru de rezistența ei în fața intimidărilor administrației și de decizia ei de a publica articolul. *Guardian* trecuse curajos și admirabil prin aceasta.

Deși mi se păruse la momentul respectiv o întârziere substanțială, este clar, retrospectiv, că *Guardian* s-a mișcat cu o viteză și un curaj remarcabile; sunt sigur că mai mult nu ar fi făcut nici una dintre organizațiile de presă de talie comparabilă. Iar Janine arătase limpede că ziarul nu avea nici o intenție de a se culca pe lauri. „Alan insistă să publicăm PRISM astăzi", a spus ea. Eu, bineînțeles, nu puteam fi mai bucuros.

Ce a făcut ca dezvăluirile PRISM să fie așa de importante a fost faptul că programul permitea NSA să obțină aproape tot ce voia de la companiile de internet pe care milioane de persoane din întreaga lume le folosesc în prezent ca principalul mijloc de comunicare. Această mișcare a fost posibilă prin legile pe care administrația SUA le implementase imediat după 11 septembrie, care învesteau NSA cu puteri extinse de a-i supraveghea pe americani și cu o autoritate aproape nelimitată de a efectua o supraveghere masivă fără discriminare a întregii populații străine.

Legea FISA modificată din 2008 este în prezent cea care guvernează supravegherea NSA. Aceasta a fost adoptată de Congresul bipartid în urma scandalului din epoca Bush privind supravegherea fără mandat efectuată de NSA, iar un rezultat cheie a fost acela că a legalizat efectiv esența programului ilegal al lui Bush. Așa cum a dezvăluit scandalul, Bush a autorizat în secret supravegherea de către NSA a americanilor și a altora în interiorul Statelor Unite, justificând ordinul prin necesitatea de a căuta activitatea teroristă. Ordinul a anulat cerința de a obține un mandat aprobat de un tribunal, necesar în mod obișnuit pentru spionajul intern, și a condus la supravegherea secretă a mii de persoane în interiorul Statelor Unite.

În pofida protestelor care susţineau că programul este ilegal, legea FISA din 2008 a căutat să instituţionalizeze o parte din schemă, nu să îi pună capăt. Legea se bazează pe o distincţie între „persoanele din SUA" (cetăţeni americani și cei care locuiesc legal pe teritoriul american) și toate celelalte persoane. Pentru a urmări direct apelurile telefonice sau e-mailurile unei persoane din SUA, NSA trebuie să obţină un mandat individual de la tribunalul FISA.

Dar pentru toate celelalte persoane, indiferent unde s-ar afla, nu este nevoie de nici un mandat individual, *nici măcar în cazul comunicării cu persoane din SUA*. În conformitate cu secţiunea 702 a legii din 2008, NSA i se cere doar ca o dată pe an să trimită tribunalului FISA liniile generale pentru determinarea ţintelor din anul respectiv – criteriul este în principal acela că supravegherea va „ajuta la strângerea legitimă de informaţii privind străinii" – și apoi primește o autorizaţie generală pentru a acţiona. Odată ce tribunalul FISA aplică ștampila „aprobat" pe aceste permise, NSA este împuternicită să aleagă ca ţintă de supraveghere orice cetăţean străin vrea și poate obliga companiile de telecomunicaţii și internet să ofere acces la toate comunicaţiile oricărui non-american, inclusiv cele cu interlocutori din SUA – chaturi Facebook, e-mailuri Yahoo!, căutări Google. Nu este nevoie să convingă tribunalul că persoana este vinovată de ceva sau că există vreun motiv pentru a privi ţinta cu suspiciune și nu este nevoie de selectarea persoanelor din SUA care ajung să fie supravegheate în acest proces.

Primul lucru pe ordinea de zi a redactorilor *Guardian* a fost să avertizeze administraţia în legătură cu intenţiile noastre de a publica povestea PRISM. Din nou, le-am dat termen limită până la sfârșitul zilei, după ora New Yorkului. Aceasta le asigura o zi întreagă pentru a transmite orice obiecţii, pentru a ne asigura că putem neutraliza inevitabilele lor plângeri că nu au avut suficient timp ca să răspundă. Dar era, de asemenea, vital să solicităm comentarii de la companiile de internet care,

potrivit documentelor NSA, furnizaseră agenţiei acces direct la serverele lor în cadrul PRISM: Facebook, Google, Apple, YouTube, Skype și celelalte.

Având ore întregi de așteptat, m-am întors în camera de hotel a lui Snowden, unde Laura lucra cu el pe diverse subiecte. La acel moment, după ce trecuserăm de un prag semnificativ – cu publicarea primei dezvăluiri explozive –, Snowden devenise în mod vizibil mai vigilent în legătură cu siguranţa sa. După ce am intrat, a pus încă o pernă la ușă. Apoi, când voia să îmi arate ceva pe computerul său, își punea o pătură în cap ca să împiedice camerele de luat vederi din tavan să îi înregistreze parolele. Când suna telefonul, îngheţam cu toţii: Cine putea suna? Snowden ridica receptorul, foarte precaut, după ce suna de câteva ori: cameristele hotelului, văzând semnul NU DERANJAŢI pe ușă, verificau să vadă dacă vrea curăţenie în cameră. „Nu, mulţumesc“, spunea el scurt.

Atmosfera era mereu tensionată atunci când ne întâlneam în camera lui Snowden, iar după ce am început publicarea tensiunea s-a amplificat. Nu știam dacă NSA a identificat sursa scurgerii de informaţii. Dacă da, știau unde este Snowden? Știau agenţii din Hong Kong sau China? Se putea ca o bătaie la ușa lui Snowden, în orice moment, să pună capăt imediat și în mod neplăcut muncii noastre împreună.

În fundal, televizorul era mereu deschis și părea că cineva vorbește mereu despre NSA. După ce a apărut povestea cu Verizon, programele de știri vorbeau aproape numai despre „colectarea masivă fără discriminare“ și „date telefonice locale“ și „abuzuri de supraveghere“. În timp ce discutam despre următoarele noastre articole, Laura și cu mine ne uitam la Snowden cum urmărește frenezia pe care o declanșase.

Apoi, la 2.00 ora Hong Kongului, când articolul despre PRISM urma să apară, am primit vești de la Janine.

„S-a întâmplat ceva extrem de ciudat“, a spus ea. „Companiile tehnologice neagă vehement ce scrie în documentele NSA. Insistă că nu au auzit niciodată despre PRISM.“

Am trecut în revistă posibilele explicaţii ale negării lor. Poate documentele NSA exagerau capacităţile agenţiei. Poate companiile tehnologice pur și simplu minţeau sau poate persoanele contactate nu știau despre aranjamentele companiei cu NSA. Sau poate PRISM era doar un nume de cod intern al NSA, neîmpărtășit vreodată cu aceste companii.

Indiferent care era explicaţia, a trebuit să rescriem articolul, nu numai ca să includem negările, ci și ca să punem accentul pe ciudata diferenţă între documentele NSA și poziţia companiilor tehnologice.

„Haide să nu luăm poziţie în privinţa cui are dreptate. Hai să prezentăm doar dezacordul și să îi lăsăm să îl rezolve în public“, am propus eu. Intenţia noastră era ca articolul să forţeze o discuţie deschisă despre ceea ce acceptase industria de internet să facă cu comunicaţiile utilizatorilor săi; dacă versiunea lor intra în conflict cu documentele NSA, vor trebui să o rezolve în văzul tuturor, așa cum ar trebui să se întâmple.

Janine a fost de acord și după două ore mi-a trimis o schiţă a articolului despre PRISM. Titlul era:

> Programul Prism al NSA interceptează datele utilizatorilor Apple, Google şi alții
>
> • Programul strict secret Prism pretinde acces direct la serverele firmelor, inclusiv Google, Apple şi Facebook
>
> • Companiile neagă că ar şti ceva despre programul care este în funcțiune din 2007

După citarea documentelor NSA care descriau PRISM, articolul preciza: „Deși prezentarea pretinde că programul se desfășoară cu asistenţa companiilor, toate cele care au răspuns solicitării *Guardian* de a comenta joi au negat că știu despre existenţa unui astfel de program“. Mie mi se părea grozav articolul, iar Janine a promis că îl va publica în jumătate de oră.

În timp ce așteptam cu nerăbdare ca minutele să treacă, am auzit sunetul de clopoţel care anunţa sosirea unui mesaj.

Speram să am o confirmare de la Janine, care să mă anunţe că articolul PRISM este încărcat. Mesajul era de la Janine, dar nu era ceea ce mă așteptam eu.

„*The Post* tocmai a publicat articolul său despre PRISM“, a spus ea.

Poftim? Voiam să știu de ce își schimbase *The Post* programul brusc pentru a trimite articolul spre publicare cu trei zile înainte de data planificată.

Laura a aflat pe scurt de la Barton Gellman că *The Post* a aflat despre intenţiile noastre după ce oficialii americani au fost contactaţi de *Guardian* în legătură cu programul PRISM în acea dimineaţă. Unul dintre acei oficiali, știind că *The Post* lucrează la un subiect similar, le-a transmis informaţia despre articolul nostru privind PRISM. *The Post* a accelerat atunci programarea pentru a evita să i se fure exclusivitatea.

Acum detestam procesul de deliberare și mai mult: un oficial american a exploatat procedura de prepublicare, ce se presupune că ar fi trebuit să protejeze securitatea naţională, pentru a se asigura că ziarul său favorit va publica povestea primul.

După ce am înghiţit informaţia, am remarcat explozia de pe Twitter în legătură cu articolul PRISM din *Washington Post*. Dar când am început să îl citesc, am văzut că lipsește ceva: contradicția dintre versiunea NSA și declaraţiile companiilor de internet.

Denumit „Serviciile de informaţii americane și britanice extrag date de la nouă companii de internet americane în cadrul unui amplu program secret“, cu semnăturile lui Gellman și a Laurei, articolul susţinea că „Agenţia de Securitate Naţională și FBI interceptează direct serverele centrale a nouă companii mari de internet, extrăgând discuţii, fotografii, e-mailuri, documente și jurnalele de conectare care le permit analiștilor să urmărească ţintele străine“. Mai semnificativ, articolul susţinea că respectivele nouă companii „participă cu bună știinţă la operaţiunile PRISM“.

Articolul nostru despre PRISM a fost publicat după zece minute, cu un accent diferit și un ton mult mai caustic, insistând în primul rând pe negările vehemente ale companiilor de internet.

Încă o dată, reacţia a fost explozivă. Mai mult, a fost internaţională. Spre deosebire de furnizori de telefonie ca Verizon, care activează, în general, într-o ţară, giganţii de internet sunt globali. Miliarde de persoane de peste tot din lume – în ţări de pe fiecare continent – folosesc Facebook, Gmail, Skype și Yahoo! ca mijloace principale de comunicare. Să afli că aceste companii au intrat în aranjamente secrete cu NSA pentru a oferi acces la comunicaţiile clienţilor lor a fost șocant la nivel global.

Iar acum oamenii începeau să speculeze că articolul anterior cu Verizon nu este un eveniment singular: cele două semnalau o serie de scurgeri de informaţii de la NSA.

Publicarea articolului despre PRISM a reprezentat ultima zi din următoarele luni în care abia am putut citi, nu mai pun la socoteală să răspund la toate e-mailurile pe care le primisem. Uitându-mă în inbox, am văzut aproape toate numele instituţiilor de presă mari din lume care voiau un interviu: dezbaterea la nivel internaţional pe care Snowden voia să o declanșeze era în desfășurare – după doar două zile de articole. M-am gândit la volumul imens de documente ce urmau, la ce va însemna acest lucru pentru viaţa mea și cum va răspunde administraţia americană odată ce își va da seama cu ce se confruntă.

Ca și în ziua precedentă, am petrecut primele ore ale dimineţii în Hong Kong în show-uri de televiziune difuzate la ore de vârf în Statele Unite. Tiparul pe care l-am urmat pe toată perioada șederii mele în Hong Kong fusese setat: lucram la articole în timpul nopţii cu *Guardian*, dădeam interviuri în presă ziua, după care mă alăturam Laurei și lui Snowden în camera de hotel a acestuia.

Am luat taxiul în mod frecvent la orele 3.00 sau 4.00, ca să merg în studiouri de televiziune, întotdeauna având în minte instrucţiunile „siguranţei operaţionale“ ale lui Snowden: să nu plec niciodată cu laptopul sau stickuri de memorie pline cu documente, ca să previn manipularea sau furtul acestora. Am mers pe străzile pustii din Hong Kong având în spate permanent un rucsac greu, indiferent unde mergeam sau la ce oră. Am luptat la fiecare pas cu paranoia și deseori m-am trezit că mă uitam peste umăr, strângându-mi mai tare rucsacul de fiecare dată când se apropia cineva.

Când terminam șirul de interviuri televizate, mă îndreptam către camera lui Snowden, unde Laura, Snowden și cu mine – uneori însoţiţi și de MacAskill – continuam să lucrăm, întrerupându-ne doar pentru a privi la televizor. Eram uimiţi de reacţia pozitivă, de cât de substanţial părea angajamentul presei faţă de aceste dezvăluiri și de cât de furioși erau majoritatea comentatorilor: nu pe cei care aduseseră transparenţa, ci pe nivelul extraordinar al supravegherii statului pe care îl dezvăluiserăm.

Acum mă simțeam în stare să pun în practică una dintre strategiile pe care le plănuisem, anume să răspund sfidător și dispreţuitor la tactica administraţiei de a invoca 11 septembrie ca justificare pentru spionajul său. Am început să denunţ acuzaţiile obosite și predictibile ale Washingtonului – că am periclitat securitatea naţională, că am ajutat terorismul, că am comis o infracţiune dezvăluind secrete naţionale.

M-am simţit impulsionat să argumentez că acestea erau strategiile transparente și manipulative ale oficialilor guvernamentali prinși făcând lucruri care îi jenau și le prejudiciau reputaţia. Astfel de atacuri nu puteau descuraja relatările noastre: vom publica mult mai multe articole din documente, fără să acordăm atenţie intimidărilor și ameninţărilor, făcându-ne datoria de jurnaliști. Am vrut să fiu clar: intimidarea și discreditarea uzuale erau zadarnice. În pofida acestei poziţii

sfidătoare, majoritatea presei, în acele prime zile, ne sprijinea munca.

Acest lucru m-a surprins pentru că, mai ales după 11 septembrie (deși chiar și înainte de această dată), presa americană, în general, fusese șovină și foarte loială administrației, și prin urmare ostilă, uneori chiar în mod răutăcios, față de oricine dezvăluia secretele acesteia.

Când WikiLeaks a început publicarea documentelor secretizate legate de războaiele din Irak și Afghanistan și în special telegramele diplomatice, apelurile la urmărirea în justiție a WikiLeaks au fost dominate chiar de jurnaliști americani, ceea ce a fost un comportament surprinzător în sine. Fiecare instituție aparent devotată transparenței în acțiunile puterii a denunțat și, în plus, a încercat să incrimineze unul dintre cele mai semnificative acte de transparență din ultimii ani. Ceea ce a făcut WikiLeaks – primind informația secretizată de la o sursă din cadrul administrației și apoi dezvăluind-o lumii – este în mod esențial ceea ce fac organizațiile media tot timpul.

Mă așteptasem ca presa americană să își îndrepte ostilitatea împotriva mea, mai ales atunci când am continuat să publicăm documente și când amploarea fără precedent a scurgerii de informații a devenit clară. Și, ca un critic aspru al jurnalismului apropiat aparatului de stat și a multora dintre membrii săi de seamă, mă gândeam că sunt un magnet natural pentru o astfel de ostilitate. Am puțini aliați în presa tradițională. Majoritatea erau persoane a căror activitate o atacasem public, frecvent și necruțător. M-am așteptat să se întoarcă împotriva mea cu cea dintâi ocazie, dar acea primă săptămână de apariții media a fost aproape un festival al iubirii, și nu numai când eram în direct.

Joi, în cea de-a cincea zi în Hong Kong, am mers în camera de hotel a lui Snowden și el a spus imediat că are vești care sunt „un pic alarmante“. Un dispozitiv de securitate conectat la internet din casa în care locuia cu iubita lui în Hawaii detectase

că două persoane din cadrul NSA – cineva care se ocupa de resurse umane și un „ofiţer de poliţie“ din cadrul NSA – veniseră să îl caute.

Snowden era aproape sigur că acest lucru însemna că NSA îl identificase ca posibila sursă a scurgerii de informaţii, dar eu eram sceptic. „Dacă ei credeau că tu ai făcut acest lucru, atunci ar fi trimis hoarde de agenţi FBI cu mandat de percheziţie și probabil echipe SWAT, nu un singur ofiţer NSA și o persoană de la resurse umane.“ Mi-am închipuit că este doar o anchetă automată și de rutină, generată în momentul în care un angajat al NSA absentează timp de câteva săptămâni fără explicaţii. Dar Snowden a sugerat că poate sunt în mod intenţionat discreţi pentru a evita să atragă atenţia presei sau pentru a începe eforturile de a suprima dovezile.

Indiferent ce însemna aceasta, sublinia necesitatea de a pregăti rapid articolul și înregistrarea video care dezvăluiau că Snowden este sursa dezvăluirilor. Eram hotărâţi ca lumea să afle despre Snowden, despre acţiunile și motivele lui, de la Snowden însuși, nu printr-o campanie de denigrare dusă de administraţia americană în timp ce el se ascundea sau era în custodie și nu se putea apăra.

Planul nostru era să mai publicăm două articole, unul vineri, a doua zi, iar altul sâmbătă. Apoi, duminică, urma să publicăm un articol lung despre Snowden, însoţit de un interviu video și de o versiune scrisă de întrebări și răspunsuri cu el, pe care să o realizeze Ewen.

Laura petrecuse deja 48 de ore la editarea înregistrării cu primul meu interviu cu Snowden, dar a spus că era prea detaliată, prea lungă și fragmentată pentru a o folosi. Voia să filmeze un nou interviu imediat, unul care să fie mai concis și mai concentrat, și a scris o listă cu aproximativ 20 de întrebări precise pe care eu să i le adresez. Am adăugat unele proprii în timp ce Laura își instala camera și ne dădea instrucţiuni unde să stăm.

„Numele meu este Ed Snowden“ începe de acum faimosul film. „Am 29 de ani. Lucrez pentru Booz Allen Hamilton ca analist de infrastructură pentru NSA în Hawaii.“

Snowden a continuat să ofere răspunsuri concise, stoice și raţionale la fiecare întrebare: De ce a decis să dezvăluie aceste documente? De ce a fost atât de important acest lucru încât să își sacrifice libertatea? Care erau cele mai semnificative dezvăluiri? Apărea ceva ilegal sau penal în aceste documente? Ce se aștepta să se întâmple cu el?

În timp ce dădea exemple de supraveghere ilegală și invazivă, a început să se însufleţească. S-a întristat doar atunci când l-am întrebat dacă se așteaptă la repercusiuni, temându-se că administraţia îi va urmări familia și iubita pentru a se răzbuna. Va evita contactul cu ei pentru a reduce riscul, a spus el, dar știa că nu îi poate proteja în totalitate. „Acesta este lucrul care mă ţine treaz noaptea, ce se va întâmpla cu ei“, a spus el, în timp ce ochii i s-au umplut de lacrimi, prima și ultima dată când am văzut întâmplându-se acest lucru.

În timp ce Laura a lucrat la editarea înregistrării video, Ewen și cu mine am finalizat următoarele două articole. Cel de-al treilea articol, publicat chiar în ziua respectivă, dezvăluia o directivă prezidenţială strict secretă semnată de președintele Obama în noiembrie 2012, care ordona Pentagonului și agenţiilor asociate să pregătească o serie de operaţiuni informatice ofensive și agresive în lume. „Oficialilor de rang înalt din cadrul securităţii naţionale și al serviciilor de informaţii“, explica primul paragraf, li s-a cerut „să întocmească o listă cu potenţiale ţinte străine pentru atacuri informatice americane, arată o directivă prezidenţială strict secretă obţinută de *Guardian*“.

Cel de-al patrulea articol, publicat așa cum planificasem, sâmbătă, era despre BOUNDLESS INFORMANT, programul NSA de urmărire, și descria rapoarte care arătau că NSA strânge, analizează și stochează miliarde de apeluri telefonice și e-mailuri trimise prin infrastructura de telecomunicaţii

americană. Acesta ridica și întrebarea dacă oficialii NSA au minţit Congresul când au refuzat să răspundă unor senatori despre numărul comunicaţiilor interne interceptate, pretinzând că nu deţin astfel de statistici și nu pot strânge astfel de date.

După ce a fost publicat articolul despre BOUNDLESS INFORMANT, eu și Laura am plănuit să ne întâlnim la hotelul lui Snowden. Înainte de a pleca din cameră, din senin, în timp ce stăteam în pat, mi-am amintit de Cincinnatus, corespondentul meu anonim de pe e-mail din urmă cu șase luni, și de faptul că mă bombardase cu solicitări de a instala PGP, astfel încât să îmi poată furniza informaţii importante. În mijlocul entuziasmului generat de tot ceea ce se întâmpla, am crezut că poate și el are să îmi furnizeze un subiect important. Neputând să îmi amintesc adresa lui de e-mail, am găsit în cele din urmă unul dintre mesajele lui mai vechi căutând după cuvinte cheie.

„Hei, vești bune“, i-am scris. „Știu că mi-a luat ceva timp, dar în cele din urmă folosesc PGP pentru e-mailuri. Așa că sunt dispus să vorbim oricând, dacă mai ești interesat.“ Am apăsat „trimite“.

La scurt timp după ce am ajuns în camera lui, Snowden mi-a spus, nu fără o urmă de ironie: „Apropo, acel Cincinnatus căruia tocmai i-ai trimis un e-mail... eu sunt“.

Mi-a luat câteva momente să procesez acest lucru și să îmi recapăt calmul. Acea persoană, care cu multe luni înainte încercase cu disperare să mă facă să folosesc programul de criptare... era Snowden. Primul meu contact cu el nu fusese în mai, ci cu multe luni în urmă. Înainte să o contacteze pe Laura în legătură cu documentele, înainte să contacteze pe oricine altcineva, el încercase să ajungă la mine.

Acum, cu fiecare zi care trecea, orele întregi pe care toţi trei le petrecuserăm împreună creaseră o legătură strânsă între noi. Stângăcia și tensiunea de la prima noastră întâlnire se transformaseră rapid într-o relaţie de colaborare, încredere

și scop comun. Știam că ne implicaserăm împreună într-unul dintre cele mai semnificative evenimente din viaţa noastră.

Dar cu articolul despre BOUNDLESS INFORMANT care se afla acum în faţa noastră, starea relativ destinsă pe care reuși-serăm să o păstrăm în precedentele zile s-a transformat într-o anxietate palpabilă: mai erau mai puţin de 24 de ore până la dezvăluirea identităţii lui Snowden și știam că aceasta va schimba totul, în primul rând pentru el. Toţi trei trăiserăm o experienţă scurtă, dar extrem de intensă și plină de satisfacţii. Unul dintre noi, Snowden, urma să fie în curând eliminat din grup, probabil să meargă la închisoare pentru o lungă perioadă de timp – un fapt care plana în mod deprimant în aer încă de la început, încărcând atmosfera, cel puţin pentru mine. Doar Snowden părea să nu fie deranjat de acest lucru. Acum, un umor macabru ameţitor se strecurase în ceea ce făceam.

„Vreau patul de jos de la Gitmo"*, a glumit Snowden contemplând perspectivele noastre. În timp ce vorbeam despre viitoarele articole, el spunea lucruri precum „Asta duce la condamnare. Singura întrebare este dacă duce la condamnarea voastră sau a mea". În cea mai mare parte a timpului a rămas însă incredibil de calm. Chiar și acum, când orele de libertate îi erau numărate, Snowden continua să meargă la culcare la 10.30, așa cum făcuse în fiecare seară cât am stat în Hong Kong.

În timp ce eu abia prindeam două ore de somn agitat la vremea respectivă, el dormea ore bune. „Bine, mă duc la culcare", anunţa el nonșalant în fiecare seară înainte de a se retrage pentru șapte ore și jumătate de somn profund, apărând complet revigorat a doua zi.

Când l-am întrebat cum poate să doarmă atât de bine în condițiile date, Snowden a spus că se simte profund împăcat cu ceea ce a făcut și astfel nopţile sunt ușoare. „Îmi dau seama

---

* Închisoarea americană Guantanamo Bay, din Cuba, înființată după atacurile teroriste de la 11 septembrie 2001 drept centru de detenție temporar și transformată după aproape doi ani în închisoare permanentă (n.red.)

că mai am puţine zile în care să beneficiez de o pernă confortabilă“, a glumit el, „așa că ar trebui să mă bucur de ele“.

Duminică după-amiaza la Hong Kong, eu și Ewen făceam ultimele revizuiri la articolul nostru care îl prezenta pe Snowden lumii întregi, în timp ce Laura termina de editat înregistrarea video. Am vorbit cu Janine, care a intrat pe chat în timp ce la New York se făcea dimineaţă, despre importanţa deosebită a modului în care trebuia tratată această știre și despre obligaţia personală pe care o simţeam faţă de Snowden de a prezenta cu atenția cuvenită alegerile lui. Ajunsesem să am încredere în colegii mei de la *Guardian* din ce în ce mai mult, atât editorial, cât și pentru curajul lor. Dar în acest caz voiam să verific orice corectură, mare sau mică, adusă articolului care urma să îl dezvăluie lumii pe Snowden.

Mai târziu în acea după-amiază din Hong Kong, Laura a venit în camera mea de hotel pentru a ne arăta filmul mie și lui Ewen. Toţi trei l-am urmărit în liniște. Munca Laurei era strălucită – filmul era gata și editarea era superbă –, dar în principal forța consta în a-l auzi pe Snowden vorbind. El și-a expus răspicat convingerile, pasiunea și forţa angajamentului care îl determinaseră să acţioneze. Curajul lui de a-și asuma faptele și responsabilitatea pentru acţiunile sale, refuzul lui de a se ascunde, cu riscul de a fi vânat, știam că vor inspira milioane de oameni.

Ceea ce voiam mai mult decât orice era ca lumea să vadă curajul lui Snowden. Administraţia americană lucrase din greu în ultimul deceniu să demonstreze puteri nelimitate. Începuse războaie, torturase și încarcerase oameni fără să îi acuze, bombardase cu avioane fără pilot ţinte, în asasinate extrajudiciare. Iar mesagerii nu erau imuni la aceasta: avertizorii de integritate fuseseră abuzaţi și urmăriţi în justiţie, jurnaliștii fuseseră ameninţaţi cu închisoarea. Printr-o expunere atent cultivată a intimidării oricui avea în vedere o provocare semnificativă, administraţia se străduise să arate oamenilor din întreaga

lume că puterea sa nu este constrânsă de lege sau etică, nici de moralitate sau Constituţie: *uite ce putem face și vom acționa astfel împotriva celor care se opun scopurilor noastre*.

Snowden sfidase intimidarea cât s-a putut de direct. Curajul este contagios. Știam că poate trezi multe persoane să facă același lucru.

La ora 14.00 pe Coasta de Est, duminică 9 iunie, *Guardian* publica articolul care îl dezvăluia lumii pe Snowden: „Edward Snowden: Avertizorul de integritate din spatele dezvăluirilor despre supravegherea NSA". La începutul articolului era filmul de 12 minute al Laurei; primul rând spunea „Persoana responsabilă de una dintre cele mai semnificative scurgeri de informaţii din istoria politică a SUA este Edward Snowden, un fost asistent tehnic pentru CIA în vârstă de 29 de ani și actual angajat al contractorului din domeniul apărării Booz Allen Hamilton". Articolul spunea povestea lui Snowden, expunea motivele sale și proclama că „Snowden va rămâne în istorie drept unul dintre cei mai importanţi avertizori de integritate, alături de Daniel Ellsberg și Bradley Manning". Am citat din primele note pe care Snowden ni le adresase mie și Laurei: „Înţeleg că voi fi făcut să sufăr pentru acţiunile mele... dar voi fi mulţumit dacă federaţia legilor secrete, iertarea inegală și puterile irezistibile ale executivului care conduc lumea pe care o iubesc vor fi dezvăluite chiar și pentru un moment".

Reacţia la articol și la film a fost mult mai intensă decât orice trăisem ca scriitor. Ellsberg însuși, scriind în ziua următoare în *Guardian*, proclama că „nu a existat o scurgere de informaţii mai mare în istoria americană ca publicarea materialelor despre NSA ale lui Edward Snowden – și aceasta include în mod clar Documentele Pentagonului din urmă cu 40 de ani".

Câteva sute de mii de persoane au postat link-ul pe paginile lor de Facebook doar în primele zile. Aproape trei milioane de persoane au urmărit interviul pe YouTube. Multe altele l-au văzut pe *Guardian* online. Răspunsul copleșitor la curajul lui Snowden a fost șoc și inspiraţie.

Laura, Snowden și cu mine am urmărit reacţia faţă de prezentarea lui împreună, în timp ce eu dezbăteam cu doi strategi media ai *Guardian* despre ce interviuri televizate să accept luni dimineaţa. Am convenit asupra *Morning Joe* de la MSNBC, urmat de *Today show* de la NBC – cele mai matinale dezbateri care urmau să modeleze relatarea despre Snowden din ziua respectivă.

Dar înainte să ajung la acele interviuri, am fost distrași de un apel telefonic la 5.00 dimineaţa – cu câteva ore după ce apăruse articolul despre Snowden – de la un vechi cititor al meu care locuiește la Hong Kong și cu care comunicasem periodic toată săptămâna. În acel apel telefonic matinal, el sublinia că toată lumea îl va căuta pe Snowden la Hong Kong și a insistat că Snowden trebuie să găsească urgent avocaţi cu relaţii în oraș. El avea de partea lui doi dintre cei mai buni avocaţi specializaţi în drepturile omului, dornici să îl reprezinte. Puteau veni toţi trei, imediat, la hotelul la care stăteam?

Am convenit să ne întâlnim un pic mai târziu, la ora 8.00. Am dormit vreo două ore până a sunat el, cu o oră înainte, la 7.00.

„Suntem deja aici“, a spus el, „la parterul hotelului tău. Îi am cu mine pe cei doi avocaţi. Lobby-ul este plin de camere de luat vederi și de reporteri. Presa caută hotelul lui Snowden și îl va găsi imediat, iar avocaţii spun că este vital să ajungă la el înainte să îl găsească presa“.

Abia trezit din somn, am aruncat pe mine primele haine pe care le-am găsit și m-am împleticit către ușă. Imediat ce am deschis, mi-au apărut în faţă flashuri de la mai multe aparate foto. Hoarda de reporteri evident că plătiseră pe cineva din personalul hotelului pentru a afla numărul camerei mele. Două femei s-au prezentat ca fiind reporteri din Hong Kong ai *Wall Street Journal*; alţii, inclusiv unul cu o cameră mare, erau de la Associated Press.

S-au repezit cu întrebări și au format un semicerc în mișcare în jurul meu în timp ce mă îndreptam spre lift. S-au înghesuit

cu mine în lift, punând întrebări una după alta, la care dădeam de cele mai multe ori replici scurte, tăioase și inutile.

Jos în lobby, un nou furnicar de camere și de reporteri s-a alăturat grupului. Am încercat să-i caut cu privirea pe cititorul meu și pe avocaţi, dar nu m-am putut mișca un metru fără să am calea blocată.

Eram deosebit de îngrijorat de mulţimea care va încerca să mă urmărească și care împiedica avocaţii să ajungă la Snowden. Până la urmă am decis să susţin o conferinţă de presă improvizată în lobby, răspunzând la întrebări astfel încât reporterii să plece. După aproximativ 15 minute, cei mai mulți s-au dispersat.

M-am simţit ușurat să dau peste Gill Phillips, avocatul-șef al *Guardian*, care s-a oprit în Hong Kong în drumul ei dinspre Australia către Londra pentru a ne oferi consiliere juridică mie și lui Ewen. Ea a spus că vrea să exploreze toate posibilele căi de care dispune *Guardian* pentru a-l proteja pe Snowden. „Alan vrea să îi ofere tot sprijinul pe care i-l putem acorda", a spus ea. Am încercat să vorbim mai mult, dar nu aveam intimitate, cu ultimii câţiva reporteri care trăgeau cu urechea.

În cele din urmă l-am găsit pe cititorul meu împreună cu cei doi avocaţi din Hong Kong pe care îi adusese cu el. Am plănuit cum să vorbim fără să fim urmăriţi și am șters-o cu toţii în camera lui Gill. Încă urmăriţi de câţiva reporteri, le-am închis ușa în faţă. Am trecut direct la afaceri. Avocaţii au vrut să urgenteze discuţia cu Snowden pentru a primi permisiunea legală de a-l reprezenta, moment din care puteau începe să acţioneze în numele lui.

Gill a dat nenumărate telefoane pentru a afla mai multe despre acești avocaţi, pe care abia îi întâlniserăm, înainte de a li-l încredinţa pe Snowden. A putut să stabilească faptul că ei erau într-adevăr cunoscuţi și renumiţi în drepturile omului și azil și că păreau destul de bine conectaţi politic în Hong Kong. În timp ce Gill își desfășura sârguincios verificarea, eu am intrat pe programul de chat. Atât Snowden, cât și Laura erau online.

Laura, care acum stătea la hotelul lui Snowden, era sigură că nu este decât o chestiune de timp până când reporterii vor găsi și hotelul lor. Snowden voia clar să plece. I-am spus despre avocaţi, care erau gata să meargă în camera lui de hotel. Snowden a spus că ar trebui să îl ia și să îl ducă într-un loc sigur. Este „timpul să intru în acea parte a planului în care cer lumii protecţie și justiţie", a spus el. „Dar trebuie să ies din hotel fără să fiu recunoscut de reporteri", a continuat el. „Altfel mă vor urmări oriunde voi merge".

Le-am transmis aceste îngrijorări avocaţilor. „Are vreo idee cum să preîntâmpine acest lucru?", a întrebat unul dintre ei.

I-am transmis întrebarea lui Snowden.

„Sunt în curs de a face niște modificări pentru a-mi schimba înfăţișarea", a spus el, fiind clar că se gândise anterior la acest lucru. „Mă pot face de nerecunoscut."

Atunci m-am gândit că avocaţii pot vorbi cu el direct. Înainte de a putea face acest lucru, ei aveau nevoie ca Snowden să rostească o frază formală despre angajarea lor. I-am trimis fraza lui Snowden și el a scris-o și mi-a trimis-o înapoi. Avocaţii au trecut apoi la computer și au început să discute cu Snowden.

După zece minute, cei doi avocaţi au anunţat că se îndreaptă către hotelul lui imediat pentru a se întâlni cu Snowden, în timp ce acesta încerca să părăsească hotelul fără să fie depistat.

„Ce intenţionaţi să faceţi cu el după aceasta?", am întrebat.

Ei ar fi vrut să îl ducă la Misiunea ONU din Hong Kong și să ceară oficial protecţia ONU faţă de administraţia SUA, pe baza faptului că Snowden este un refugiat care cere azil. Sau vor încerca să îi găsească o „casă conspirativă", au spus ei.

Dar cum să scoţi avocaţii din hotel fără să fii urmărit? Am improvizat un plan: voi ieși din cameră împreună cu Gill și voi coborî în lobby pentru a ademeni reporterii care încă așteptau în faţa ușii noastre. Avocaţii vor aștepta apoi câteva minute și vor ieși din hotel, sperând să nu fie observaţi.

Șiretlicul a mers. După 30 de minute de discuţie cu Gill într-un mall din cadrul hotelului, m-am întors în camera mea și l-am sunat nerăbdător pe unul dintre avocaţi pe mobil.

„A ieșit chiar înainte ca jurnaliștii să înceapă să se adune la parter“, a spus el. „Ne-am întâlnit cu el în camera lui de hotel și apoi am traversat pasarela către un mall“ – în faţa camerei cu crocodilul, unde ne-am întâlnit pentru prima dată cu Snowden, am aflat eu mai târziu – „și apoi am urcat în mașina care ne aștepta. Acum este cu noi“.

Unde îl duceau?

„Este mai bine să nu vorbim despre acest lucru la telefon“, a replicat avocatul. „Va fi în siguranţă pentru moment.“

M-am simţit foarte ușurat că Snowden este pe mâini bune, dar știam că sunt șanse mari să nu ne mai vedem vreodată sau să mai vorbesc cu el, cel puţin nu ca om liber. Cel mai probabil, m-am gândit, îl vom vedea următoarea dată la televizor, îmbrăcat în uniforma portocalie de deținut și purtând cătușe, într-o sală de tribunal din SUA, fiind acuzat de spionaj.

În timp ce mă obișnuiam cu ideea, cineva mi-a bătut la ușă. Era managerul general al hotelului care venise să îmi spună că telefonul sună fără încetare în camera mea (le dădusem instrucţiuni celor de la recepţie să blocheze toate apelurile). Erau, de asemenea, o mulțime de reporteri, fotografi și cameramani în lobby, așteptând să apar.

„Dacă vreţi“, mi-a spus, „vă putem scoate cu un lift din spate și apoi pe la o ieșire unde nu o să vă vadă nimeni. Iar avocatul *Guardian* a făcut o rezervare pentru dumneavoastră la un alt hotel, sub un nume diferit, dacă asta vreţi să faceţi“.

Era clar ce voia managementul hotelului: *vrem să pleci din cauza scandalului pe care îl creezi*. Știam însă că este o idee bună, în orice caz. Voiam să continui să lucrez într-o oarecare intimitate și încă mai speram să menţin contactul cu Snowden. Așa că mi-am făcut bagajele, l-am urmat pe manager către ieșirea din spate, m-am întâlnit cu Ewen într-o mașină care aștepta

și apoi m-am cazat la un alt hotel sub numele avocatului *Guardian*.

Primul lucru pe care l-am făcut a fost să intru pe internet, sperând să aflu ceva despre Snowden. După câteva minute, a apărut online.

„Sunt bine“, mi-a spus. „Într-o casă conspirativă deocamdată. Dar nu am nici o idee cât de sigură este sau pentru cât timp voi fi aici. Va trebui să mă mut din loc în loc, iar accesul meu la internet este nesigur, așa că nu știu când sau cât de des voi fi online.“

Era în mod evident reticent în a-mi oferi orice detalii despre locul unde se afla, iar eu nu le voiam. Știam că posibilitatea ca eu să fiu implicat în ascunderea lui era foarte limitată. Era acum cel mai căutat om din lume de către cel mai puternic guvern din lume. Statele Unite ceruseră deja autorităţilor din Hong Kong arestarea și predarea lui americanilor.

Așa că am vorbit scurt și vag, exprimându-ne speranţa că vom menţine contactul. I-am spus să rămână în siguranţă.

*

Când am mers în cele din urmă la studio pentru interviuri la *Morning Joe* și *Today show*, am remarcat imediat că sensul interviului se schimbase semnificativ. Mai degrabă decât să trateze cu mine ca reporter, gazda a preferat să atace o ţintă nouă: pe Snowden însuși, acum o figură fantomatică din Hong Kong. Mulţi jurnaliști americani și-au reluat rolul lor obișnuit de servitori ai administraţiei. Povestea nu mai era că reporterii dezvăluiseră abuzuri grave ale NSA, ci că un american care lucra pentru administraţie și-a „trădat“ obligaţiile, a comis infracţiuni și apoi „a fugit în China“.

Interviurile mele cu ambii moderatori, Mika Brzezinski și Savannah Guthrie, au fost caustice și acerbe. Nedormit de mai mult de o săptămână, nu aveam răbdare pentru criticile aduse lui Snowden încorporate în întrebările lor; eram de părere că

jurnaliștii ar trebui să îl elogieze, nu să îl demonizeze pe cineva care a adus mai multă transparenţă asupra securităţii naţionale a statului decât oricine altcineva de-a lungul multor ani.

După alte câteva zile de interviuri, am decis că este timpul să plec din Hong Kong. În mod clar, avea să-mi fie imposibil să mă întâlnesc sau să îl ajut pe Snowden rămânând acolo, într-un moment în care eram complet epuizat fizic, emoţional și psihic. Eram nerăbdător să mă întorc la Rio.

M-am gândit să zbor către New York și să mă opresc pentru o zi ca să dau interviuri – doar pentru a clarifica ce pot. Dar am fost sfătuit de un avocat să nu fac acest lucru, argumentând că nu are sens să îmi asum riscuri legale de acest fel până nu știm cum plănuiește administraţia să reacţioneze. „Tocmai ai făcut posibilă cea mai mare scurgere de informaţii despre securitatea naţională din istoria SUA și ai mers peste tot la televiziune cu cel mai sfidător mesaj posibil“, a spus el. „Va avea rost să plănuiești o călătorie în SUA după ce ne vom da seama de răspunsul Departamentului de Justiţie“.

Nu am fost de acord; eram de părere că este extrem de improbabil ca administraţia Obama să aresteze un jurnalist în mijlocul unui astfel de subiect. Dar eram mult prea epuizat ca să mă cert sau să îmi asum riscul. Așa că *Guardian* mi-a cumpărat biletul de întoarcere la Rio prin Dubai, departe de Statele Unite. Pentru moment, m-am gândit eu, făcusem destule.

Capitolul 3
Colectează tot

Arhiva de documente pe care Snowden le adunase era uimitoare atât ca număr, cât și ca anvergură. Chiar și pentru cineva care își petrecuse ani întregi scriind despre pericolele supravegherii secrete a SUA, amploarea reală a sistemului de spionare era pur și simplu șocantă, cu atât mai mult cu cât fusese clar implementat aproape fără nici o responsabilitate, fără transparenţă și fără limite.

În ceea ce privește miile de programe discrete de supraveghere descrise de arhivă, cei care le implementaseră nu intenţionau ca acestea să devină publice. Multe programe erau îndreptate împotriva populaţiei americane, dar zeci de ţări de pe planetă – inclusiv democraţii considerate în mod tradiţional aliaţi ai SUA, precum Franţa, Brazilia, India și Germania – erau, de asemenea, vizate de supravegherea în masă fără discriminare.

Arhiva lui Snowden era organizată elegant, dar mărimea și complexitatea ei o făceau extrem de greu de procesat. Zeci de mii de documente NSA pe care le conţinea fuseseră produse de aproape fiecare unitate și subdiviziune a agenţiei, dar arhiva conţinea unele dosare de la agenţii de spionaj străine raliate. Documentele erau recente: majoritatea din 2011 și 2012 și multe din 2013. Unele erau datate chiar martie și aprilie 2013, cu doar câteva luni înainte ca noi să ne întâlnim cu Snowden la Hong Kong.

Majoritatea dosarelor din arhivă erau marcate „strict secret". Cele mai multe purtau inițialele „FVEY", ceea ce însemna că erau aprobate pentru a fi distribuite doar celor patru aliaţi apropiaţi ai NSA în programul de supraveghere, alianţa

vorbitoare de engleză „Five Eyes“ [„Cinci Ochi“] - compusă din Marea Britanie, Canada, Australia și Noua Zeelandă. Altele, destinate a fi cunoscute doar de SUA, erau marcate „NOFORN“, acronim de la „no foreign distribution“ [interzisă distribuirea externă]. Unele documente, precum ordinul tribunalului FISA care permitea colectarea înregistrărilor telefonice și directiva prezidenţială a lui Obama de pregătire a unor operaţiuni informatice ofensive, se aflau printre secretele cel mai bine păzite de administraţia SUA.

Descifrarea arhivei și limbajul NSA au implicat o curbă de învăţare abruptă. Agenţia comunică în interior și cu partenerii săi într-un limbaj specific, un jargon birocratic și pompos, uneori lăudăros și chiar dispreţuitor. Majoritatea documentelor erau destul de tehnice, pline de acronime prohibitive și nume de cod, iar uneori necesitau citirea prealabilă a altor documente pentru a fi înţelese.

Dar Snowden anticipase problema, oferind glosare de acronime și nume de programe, precum și dicţionare interne ale agenţiei pentru termenii specifici. Cu toate acestea, unele documente erau de nepătruns la prima, a doua sau chiar a treia lectură. Semnificaţia lor a reieșit doar după ce am pus cap la cap diverse părţi ale altor documente și m-am consultat cu unii dintre cei mai importanţi experţi din lume în supraveghere, criptografie, activităţi de hacking, istoria NSA și cadrul legal al spionajului american.

Dificultatea consta în faptul că munţii de documente erau deseori organizaţi nu după subiect, ci după ramura agenţiei de unde proveneau, și dezvăluirile spectaculoase erau amestecate cu o cantitate mare de material foarte tehnic sau banal. Deși *Guardian* elaborase un program de căutare în dosare după cuvinte cheie, care a fost de mare ajutor, acesta era departe de a fi perfect. Procesul de analizare a arhivei era dureros de încet, iar la multe luni după ce primiserăm documentele, unii termeni și programe încă necesitau relatări suplimentare înainte de a putea fi dezvăluiţi în siguranţă și coerent.

În pofida acestor probleme, dosarele lui Snowden dezvăluiau o ţesătură complexă de supraveghere îndreptată în mod egal împotriva americanilor (care sunt în mod explicit dincolo de misiunea NSA) și a non-americanilor. Arhiva a dezvăluit mijloacele tehnice folosite la interceptarea comunicaţiilor: pătrunderea NSA în servere de internet, sateliţi, cabluri de fibră optică subacvatice, sisteme de telefonie locale și străine și computere personale. Aceasta a identificat indivizi vizaţi de forme extrem de invazive de spionaj, o listă care conţinea de la teroriști și suspecţi de infracţiuni la lideri aleși democratic în ţările aliate și chiar cetăţeni americani obișnuiți. Și scotea la lumină strategiile globale ale NSA și scopurile sale.

Snowden plasase documentele cruciale, centrale la începutul arhivei, marcându-le ca foarte importante. Aceste dosare dezvăluiau raza de acţiune extraordinară a agenţiei, precum și înșelăciunea și chiar infracţionalitatea sa. Programul BOUNDLESS INFORMANT era una dintre primele dezvăluiri, care arăta că NSA contabilizează toate apelurile telefonice și e-mailurile colectate în fiecare zi din lumea întreagă cu o exactitate matematică. Snowden plasase aceste dosare atât de vizibil nu numai pentru că ele cuantificau volumul apelurilor telefonice și al e-mailurilor colectate și stocate de NSA – miliarde în fiecare zi –, ci și pentru că dovedeau că șeful NSA, Keith Alexander, și alţi oficiali minţiseră Congresul. În mod repetat, oficialii NSA pretinseseră că nu pot oferi cifre exacte – de fapt chiar datele pe care BOUNDLESS INFORMANT fusese conceput să le colecteze.

Timp de o lună, începând cu 8 martie 2013, de exemplu, un slide al prezentării BOUNDLESS INFORMANT arăta că o singură unitate a NSA, Operaţiuni cu Acces Global, colectase nu mai puţin de trei miliarde de apeluri telefonice și e-mailuri care trecuseră prin sistemul de telecomunicaţii american. („DNR" sau „Dialed Number Recognition" [„Recunoașterea Numărului Apelat"] se referă la apelurile telefonice; „DNI" sau „Digital Network Intelligence" [„Informaţii privind Reţeaua Digitală"]

se referă la comunicaţiile prin internet, cum ar fi e-mailurile.) Aceasta depășește colectarea efectuată de sistemele din Rusia, Mexic și aproape toate ţările din Europa și este aproximativ egală cu colectarea datelor de către China.

Per total, în doar 30 de zile, unitatea colectase date despre nu mai puţin de 97 de miliarde de e-mailuri și 124 de miliarde de apeluri telefonice din întreaga lume. Un alt document al BOUNDLESS INFORMANT detalia datele internaţionale colectate într-o perioadă de 30 de zile din Germania (500 de milioane), Brazilia (2,3 miliarde) și India (13,5 miliarde). Alte dosare arătau colectarea metadatelor în cooperare cu guvernele Franţei (70 de milioane), Spaniei (60 de milioane), Italiei (47 de milioane), Olandei (1,8 milioane), Norvegiei (33 de milioane) și Danemarcei (23 de milioane).



În pofida faptului că, prin statutul său, NSA se concentrează pe „informaţiile externe“, documentele au confirmat că publicul american a fost o ţintă la fel de importantă pentru supravegherea secretă. Nimic nu a făcut acest lucru mai clar decât un ordin secret din 25 aprilie 2013 al tribunalului FISA care cerea Verizon să predea NSA toate informaţiile despre apelurile telefonice ale clienţilor săi americani, „metadatele de telefonie“. Marcat „NOFORN“, limbajul ordinului era pe cât de clar pe atât de categoric:

> PRIN PREZENTA SE ORDONĂ ca Custodele Datelor să prezinte Agenției de Securitate Națională (NSA) pe baza

```
acestui Ordin şi să continue să prezinte
zilnic pe toată durata acestui Ordin,
cu excepția unei solicitări contrare
din partea Curții, o copie electronică
a următoarelor lucruri tangibile: toate
înregistrările detaliilor apelurilor
telefonice sau „metadatele de telefonie”
create de Verizon pentru comunicații
(i) între Statele Unite şi străinătate
sau (ii) integral în Statele Unite,
inclusiv apelurile telefonice locale.
Metadatele de telefonie includ informații
de rutare a comunicațiilor globale,
incluzând, dar fără a se limita la
sesiuni de identificare a informațiilor
(de exemplu, numărul de telefon care
inițiază sau încheie apelul, numărul de
Identitate Internațională a Abonatului
Mobil (IMSI), numărul de Identitate
Internațională a Echipamentului Mobil
(IMEI) etc.), identificatorul magistralelor
comune, numere de cartele telefonice şi
momentul şi durata apelului.
```

Acest program de colectare telefonică în masă a fost una dintre cele mai semnificative descoperiri dintr-o arhivă stufoasă cu toate tipurile de programe de supraveghere sub acoperire – de la cel pe scară largă PRISM (ce presupune colectarea datelor direct de la serverele celor mai mari companii de internet din lume) și PROGRAMUL BULLRUN, un efort comun între NSA și serviciul omolog britanic, Cartierul General pentru Comunicaţii al Guvernului (GCHQ), pentru a învinge cele mai comune forme de criptare folosite pentru protejarea tranzacţiilor online, la acţiuni la scară mai mică ale căror nume reflectă spiritul dispreţuitor și lăudăros al supremaţiei din spatele lor: GIRAFA EGOISTĂ, care vizează browserul Tor conceput să permită anonimitatea în timpul navigării online; MUSCULAR, un mijloc de a invada reţelele private ale Google și Yahoo!; OLYMPIA, programul Canadei de supraveghere a Ministerului Minelor și Energiei din Brazilia.

O parte din supraveghere a fost dedicată ostentativ suspecţilor de terorism. Dar mare parte din programe nu aveau în mod evident nimic de-a face cu securitatea naţională. Documentele îndepărtau orice urmă de îndoială că NSA era implicată și în spionaj economic, spionaj diplomatic și supravegherea întregii populaţii, în lipsa oricărei suspiciuni.

Luată în întregime, arhiva lui Snowden a condus la o ultimă concluzie simplă: administraţia SUA construise un sistem care avea ca scop să elimine complet intimitatea electronică în întreaga lume. Departe de vreo hiperbolă, acesta este literal și explicit scopul declarat al supravegherii realizate de stat: să colecteze, să depoziteze și să analizeze toate comunicaţiile electronice ale tuturor oamenilor de pe planetă. Agenţia este dedicată unei singure misiuni cuprinzătoare: să împiedice și cel mai mic element al comunicaţiilor electronice să iasă de sub controlul său sistemic.

Mandatul său autoimpus necesită o expansiune fără limite a razei de acţiune a NSA. În fiecare zi, NSA lucrează pentru identificarea comunicaţiilor electronice care nu sunt colectate și stocate și apoi dezvoltă noi tehnologii și metode pentru a remedia deficienţa. Agenţia se vede ca neavând nevoie de nici o justificare pentru a colecta orice comunicaţie electronică particulară, de nici o bază pentru a-și privi ţintele cu suspiciune. Ceea ce NSA numește „SIGINT“ – interceptarea tuturor semnalelor – este ţinta sa. Și simplul fapt că are capacitatea de a colecta aceste comunicaţii a devenit un motiv pentru a face acest lucru.

O ramură militară a Pentagonului, NSA este cea mai mare agenţie de spionaj din lume, majoritatea activităţii sale de supraveghere fiind desfășurată prin alianţa Five Eyes. Până în primăvara lui 2014, când controversa cu privire la poveștile lui Snowden a devenit tot mai intensă, agenţia a fost condusă de generalul cu patru stele Kieth B. Alexander, care a supervizat-o în ultimii nouă ani, sporind agresiv amploarea și influenţa NSA

în timpul mandatului său. În acest proces, Alexander a devenit ceea ce reporterul James Bamford a descris drept „cel mai puternic șef al unui serviciu de spionaj din istoria americană“.[1]

NSA „era deja un monstru al informaţiilor când Alexander a preluat conducerea“, a subliniat reporterul *Foreign Policy* Shane Harris, „dar sub supravegherea sa, scara și ambiţia misiunii sale s-au extins dincolo de orice preconizaseră vreodată predecesorii săi“. Niciodată înainte „o agenţie a administraţiei americane nu avusese capacitatea, precum și autoritatea legală de a colecta și de a stoca atât de multe informaţii electronice“. Un fost oficial din cadrul administraţiei care a lucrat cu șeful NSA i-a spus lui Harris că „strategia lui Alexander“ era clară: „Trebuie să am toate informaţiile“.[2] Și, a adăugat Harris, „vrea să le deţină cât de mult poate“.

Mottoul personal al lui Alexander, „Colectează tot“, transmite perfect scopul central al NSA. El a pus pentru prima dată în practică această filosofie în 2005, în timpul colectării informaţiilor provenite din interceptarea semnalelor în legătură cu ocuparea Irakului. Așa cum relata *Washington Post*[3] în 2013, Alexander era nemulţumit de limitele de funcţionare ale serviciului de contrainformaţii militare american, care urmărea doar insurgenţii suspecţi și alte ameninţări pentru forţele americane, o abordare pe care nou-numitul șef al NSA o vedea ca fiind prea constrângătoare. „El voia totul: fiecare mesaj tastat de un irakian, fiecare apel telefonic și e-mail care putea fi aspirat de puternicele computere ale agenţiei.“ Așa că administraţia a dezvoltat metode tehnologice care să colecteze toate datele privind comunicaţiile, fără discriminare, de la întreaga populaţie irakiană.

Alexander a plănuit apoi să aplice acest sistem de supraveghere totală – creat iniţial pentru populaţia străină din zona activă de război – la toţi cetăţenii americani. „Și, așa cum a făcut în Irak, Alexander a făcut presiuni pentru a obţine tot ceea ce se putea“, a relatat *The Post*: „instrumente, resurse și autoritatea legală de a colecta și de a stoca vaste cantităţi

de informaţie brută din comunicaţiile străine și americane. Astfel, „în cei opt ani la conducerea agenţiei de supraveghere electronică a ţării, Alexander, în vârstă de 61 de ani, a prezidat tăcut o revoluţie a abilităţii administraţiei de a aduna informaţii în numele securităţii naţionale“.

Reputaţia lui Alexander ca extremist al suprevegherii este bine documentată. Descriind „eforturile sale depline, la limita legalității, de a construi mașinăria perfectă de spionaj“, *Foreign Policy* l-a numit „cowboy-ul NSA“. Chiar și șeful CIA și NSA din perioada lui Bush, generalul Michael Hayden – care a supravegheat implementarea programului ilegal de supraveghere fără mandat al lui Bush și este cunoscut pentru militarismul său agresiv – a avut deseori „dureri de cap“ cu abordarea de tipul „nimic interzis“ a lui Alexander, potrivit *Foreign Policy*. Un fost oficial al serviciilor de spionaj a caracterizat viziunea lui Alexander astfel: „Să nu ne facem griji în privinţa legii. Ci să vedem cum facem ca să ne îndeplinim misiunea“. *The Post* menţionează, în mod similar, că „până și apărătorii lui susţin că agresivitatea lui Alexander l-a împins uneori în afara autorităţii sale legale“.

Deși unele dintre cele mai extreme declaraţii făcute de Alexander – cum ar fi întrebarea lui sinceră „De ce nu putem colecta toate semnalele, tot timpul?“, pe care ar fi adresat-o în 2008 în timpul unei vizite la GCHQ din Marea Britanie – au fost negate de purtătorii de cuvânt ai agenţiei ca glume scoase din context, documentele agenţiei demonstrează că Alexander nu glumea. O prezentare strict secretă de la conferinţa anuală din 2011 a alianţei Five Eyes, de exemplu, arată că NSA a îmbrăţișat explicit mottoul lui Alexander privind omniștiinţa ca principal scop al său:



Un document din 2010 prezentat la conferinţa Five Eyes de către GCHQ – referitor la programul său în desfășurare de interceptare a comunicaţiilor prin satelit, cu numele de cod TARMAC – arată clar că agenţia britanică de spionaj folosește de asemenea această sintagmă pentru a-și descrie misiunea:



Chiar și notele interne ale NSA invocă sloganul pentru a justifica extinderea capacităţilor agenţiei. O notă datată 2009 din partea directorului tehnic al Operaţiunilor Misiunii NSA,

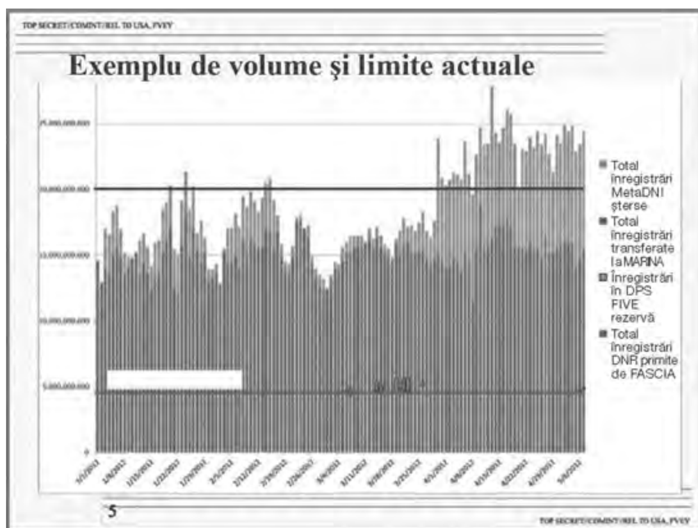
de exemplu, laudă recentele îmbunătăţiri la sediul agenţiei de colectare a datelor din Misawa, Japonia:

Planuri Viitoare (U)

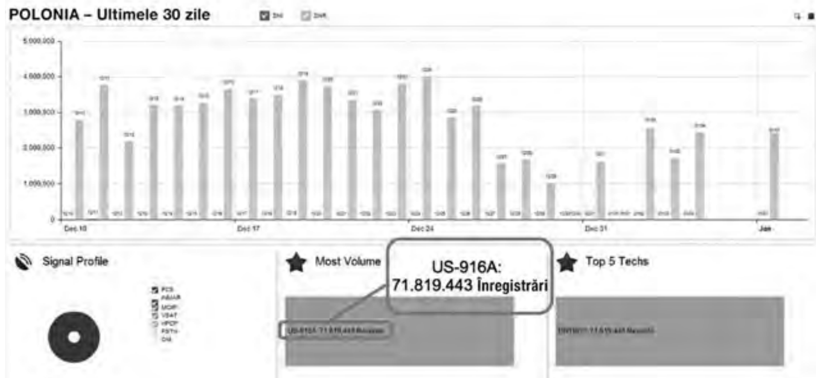
(TS//SI//REL) Pe viitor, MSOC speră să extindă numărul platformelor WORDGOPHER pentru a permite demodularea a mii de furnizori adiţionali de nivel scăzut.

Aceste ţinte sunt potrivite la modul ideal pentru demodulare software. În plus, MSOC a dezvoltat o capacitate de scanare automată şi demodulare a semnalelor pe măsură ce acestea se activează pe sateliţi. Există o multitudine de posibilităţi, care aduc misiunea noastră cu un pas mai aproape de „colectarea a tot ce se poate“.

Departe de a fi o glumă frivolă, „colectează tot“ definește aspiraţia NSA și este un scop pe care NSA este tot mai aproape de a-l atinge. Cantitatea de apeluri telefonice, e-mailuri, discuţii online, activităţi online și metadate telefonice colectate de agenţie este uimitoare. Așa cum arată un document din 2012, NSA „colectează frecvent mult mai mult conţinut decât le este folositor în mod obișnuit analiștilor“. La jumătatea lui 2012, agenţia procesa peste 20 de miliarde de evenimente comunicaţionale (atât de pe internet, cât și telefonice) din întreaga lume *în fiecare zi*:



Pentru fiecare ţară în parte, NSA produce o defalcare cotidiană, cuantificând numărul apelurilor și al e-mailurilor colectate. Graficul de mai jos, pentru Polonia, arată peste trei milioane de apeluri telefonice în unele zile, într-o perioadă de 30 de zile fiind înregistrate în total 71 de milioane:

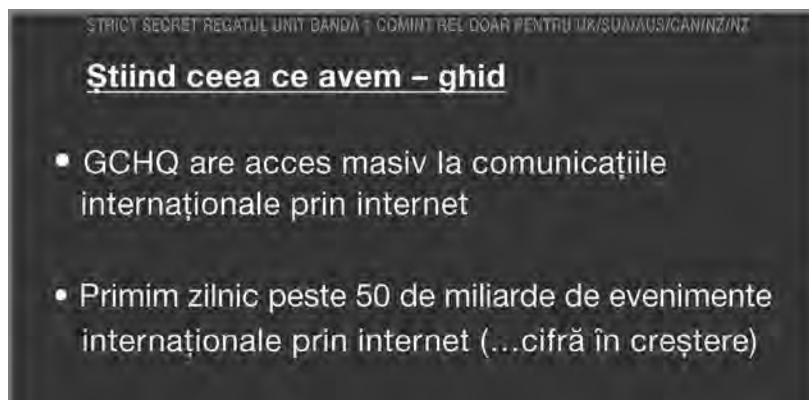


Totalul datelor interne colectate de NSA este de asemenea uimitor. Chiar înainte de dezvăluirile lui Snowden, *Washington Post* relata în 2010[4] că „în fiecare zi, sistemele de colectare ale Agenţiei de Securitate Naţională interceptează și stochează 1,7 miliarde de e-mailuri, apeluri telefonice și alte tipuri de comunicaţii" ale americanilor. William Binney, un matematician care a lucrat pentru NSA timp de trei decenii și a demisionat în urma atentatelor din 11 septembrie ca semn de protest faţă de concentrarea agenţiei tot mai mult pe intern, a făcut de asemenea numeroase declaraţii despre cantitatea de date colectate din SUA. Într-un interviu din 2012 pentru *Democracy Now!*[5], Binney a spus că „adunau de ordinul a 20 de trilioane de tranzacţii despre cetăţeni americani cu alţi cetăţeni americani".

După dezvăluirile lui Snowden, *Wall Street Journal* a relatat că sistemul de interceptări per ansamblu al NSA „are capacitatea de a ajunge la aproape 75% din traficul pe internet din SUA în căutare de informaţii străine, inclusiv o arie extinsă de comunicaţii ale străinilor și americanilor".[6] Vorbind sub

acoperirea anonimatului, actuali și foști oficiali ai NSA au declarat pentru *Journal* că, în unele cazuri, NSA „reţine conţinutul scris al e-mailurilor trimise între cetăţeni în interiorul SUA și filtrează de asemenea apelurile telefonice interne iniţiate prin internet“.

GCHQ din Marea Britanie colectează în mod similar o cantitate de date de comunicaţii atât de mare, încât abia poate stoca ceea ce are. Așa cum arată un document din 2011 realizat de britanici:



Atât de obsedată este NSA de colectarea tuturor informaţiilor, încât arhiva lui Snowden este presărată cu note interne festive care anunţă etape semnificative în procesul de colectare. Această intrare din decembrie 2012 dintr-un mesaj intern, de exemplu, proclamă cu mândrie că programul SHELLTRUMPET a procesat înregistrarea cu numărul un trilion:

(S//SI//REL PENTRU SUA, FVEY) SHELLTRUMPET procesează metadata cu numărul un trilion

De NUME REDACTAT la 2012-12-31 0738

(S//SI//REL PENTRU SUA, FVEY) În data de 21 decembrie 2012, SHELLTRUMPET a procesat metadata cu numărul un trilion. SHELLTRUMPET a început ca un analizator de metadate aproape în timp real la 8 decembrie 2007, pentru un sistem de colectare CLASIC. În cinci ani de existență, numeroase alte sisteme din Agenție au ajuns să folosească capacitățile de procesare ale SHELLTRUMPET

```
pentru o monitorizare performantă, alertarea directă prin e-mail cu privire la
un indiciu, indicii TRAFFICTHIEF, filtrul și absorbția Portal Regional în Timp
Real (RTRG). Deși a fost nevoie de cinci ani pentru a ajunge la pragul de un
trilion, aproape jumătate din acest volum a fost procesată în acest an
calendaristic, iar jumătate din acest volum a fost din DANCINGOASIS al SSO.
SHELLTRUMPET procesează în prezent două miliarde de apeluri pe zi din sistemele
SSO (sistemele active Ram-M, OAKSTAR, MYSTIC și NCSC), MUSKETEER și Second
Party. Îi vom extinde raza de acțiune la alte sisteme SSO în cursul lui 2013.
Cele un trilion de înregistrări procesate au produs peste 35 de milioane
de informații pentru TRAFFICTHIEF.
```

*

Pentru a colecta o cantitate atât de vastă de comunicaţii, NSA se bazează pe o multitudine de metode. Acestea includ interceptarea directă a cablurilor de fibră optică (inclusiv cele submarine) folosite pentru transmiterea comunicaţiilor internaţionale; redirecţionarea mesajelor către sistemul de stocare al NSA în momentul în care acestea traversează sistemul american, așa cum se întâmplă cu majoritatea comunicaţiilor din lume; și cooperarea cu serviciile de informaţii din alte ţări. Cu o frecvenţă tot mai mare, agenţia se bazează pe companiile de internet și telecomunicaţii, care transmit în mod obligatoriu informaţiile pe care le-au colectat despre clienţii lor.

Deși NSA este oficial o agenţie publică, ea are nenumărate parteneriate simultane cu corporaţii din sectorul privat și multe dintre principalele sale funcţii au fost externalizate. NSA în sine are aproximativ 3 000 de angajaţi, dar agenţia are contracte pentru aproximativ 6 000 de angajaţi ai unor corporaţii private, care deseori furnizează servicii esenţiale. Snowden însuși nu a fost angajat al NSA, ci al Dell Corporation și al contractorului din domeniul apărării Booz Allen Hamilton. Cu toate acestea, el, la fel ca mulţi colaboratori privaţi, au lucrat în birourile NSA, în funcţiile sale de bază, cu acces la secretele sale.

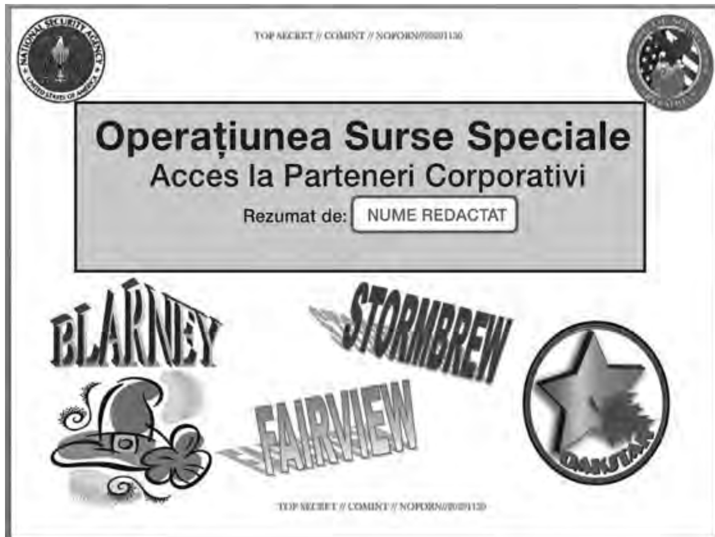
Potrivit lui Tim Shorrock, care a relatat îndelung despre relaţiile NSA cu corporaţiile, „70% din bugetul serviciilor noastre de informaţii este cheltuit pe sectorul privat“. Atunci când Michael Hayden a spus că „cea mai mare concentrare a puterii

cibernetice de pe planetă este la intersecția dintre Baltimore Parkway și Maryland Route 32", Shorrock a subliniat că „nu se referă la NSA în sine, ci la parcul de afaceri situat la aproape o milă de clădirea gigantică neagră care găzduiește sediul NSA din Fort Meade, Maryland. Aici, toți contractorii majori ai NSA, de la Booz la SAIC și Northrop Grumman, își desfășoară activitatea de supraveghere și de colectare de informații pentru agenție".

Aceste parteneriate corporative se extind dincolo de contractori pentru activitatea de colectare de informații și apărare, incluzând cele mai mari și mai importante companii de internet și de telecomunicații din lume, mai exact acele companii care controlează cea mai mare parte a comunicațiilor mondiale și pot facilita accesul la discuțiile private. După descrierea misiunilor agenției de „Apărare (Protejarea sistemelor de telecomunicații și computerizate ale SUA împotriva exploatării)" și „Ofensivă (Interceptarea și exploatarea semnalelor străine)", un document strict secret al NSA enumeră câteva dintre serviciile oferite de astfel de corporații:

Aceste parteneriate corporative, care oferă sisteme și accesul pe care se bazează NSA, sunt gestionate de unitatea strict secretă Operaţiunea Surse Speciale [SSO], o divizie care supraveghează parteneriatele corporative. Snowden a descris SSO drept „bijuteria coroanei" organizaţiei.

BLARNEY [Vorbe mieroase], FAIRVIEW [Imagine fidelă], OAKSTAR [Stea de stejar] și STORMBREW [Nori de furtună] sunt câteva dintre programele de supraveghere ale SSO în cadrul portofoliului său Acces la Parteneri Corporativi [CPA].



În cadrul acestor programe, NSA exploatează accesul la unele dintre companiile de telecomunicaţii care au sisteme internaţionale și care au intrat astfel în contact cu firme de telecomunicaţii străine pentru a-și construi, menţine și moderniza reţelele. Companiile americane redirecţionează apoi datele comunicaţiilor ţării vizate către sistemele de stocare ale NSA.

Scopul central al BLARNEY este descris de una dintre notele de informare ale NSA:

Relații & Autorități

- Folosirea parteneriatelor corporative pentru a obține acces la cablurile de fibră optică internaționale de mare capacitate, switchuri și/sau routere din întreaga lume

BLARNEY se bazează în primul rând pe o relaţie anume[8] – un vechi parteneriat cu AT&T Inc., potrivit relatărilor despre program ale *Wall Street Journal*. Conform documentelor NSA, în 2010 lista ţărilor vizate de BLARNEY includea Brazilia, Franţa, Germania, Grecia, Israel, Italia, Japonia, Mexic, Coreea de Sud și Venezuela, precum și Uniunea Europeană și Naţiunile Unite.

FAIRVIEW, un alt program al SSO, colectează ceea ce NSA se laudă a fi „cantităţi masive de date" din toată lumea. Și acesta se bazează în principal pe un singur „partener corporativ" și, în special, pe accesul acelui partener la sistemul de telecomunicaţii al naţiunilor străine. Rezumatul intern al NSA asupra FAIRVIEW este simplu și clar:

Aspecte unice

Acces la o cantitate masivă de date

Controlat de diferite autorități legale

Accesul este controlat aproape în totalitate de partener



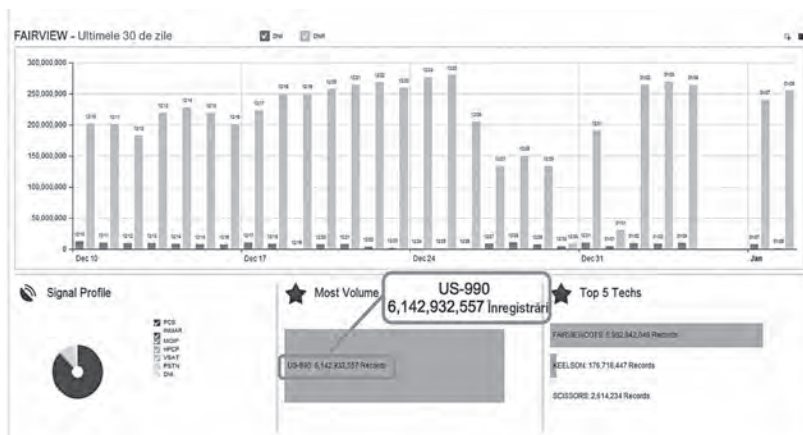
Potrivit documentelor NSA, FAIRVIEW se numără „printre primele cinci surse ale NSA de colectare a informaţiilor pentru producţie în serie“ – însemnând supraveghere continuă – „și este unul dintre cei mai mari furnizori de metadate“. Faptul că se bazează în mod covârșitor pe o singură companie de telecomunicaţii este demonstrat de afirmaţia sa că „aproximativ 75% din raportări provin dintr-o singură sursă, reflectând accesul unic de care se bucură programul la o mare varietate de comunicaţii ţintă“. Deși compania nu este menţionată, o descriere a partenerului FAIRVIEW arată clar dorinţa acestuia de a coopera:

> FAIRVIEW – Partener corporativ din 1985 cu acces la cabluri internaţionale, routere și switchuri. Partenerul operează în SUA, dar are acces la informaţii care tranzitează teritoriul naţiunii și prin relaţiile sale corporative oferă acces unic la alte companii de telecomunicaţii și ISP*. Implicat în mod agresiv în configurarea traficului pentru a transmite semnalele de interes către instrumentele noastre de monitorizare.

Graţie unei astfel de cooperări, programul FAIRVIEW colectează cantităţi vaste de informaţii despre apelurile telefonice. Un grafic, care acoperă o perioadă de 30 de zile începând cu 10 decembrie 2012, arată că acest program este responsabil de colectarea a circa 200 de milioane de înregistrări în fiecare

* Furnizori de servicii de internet (n.tr.)

zi din luna respectivă, ajungând la un total de peste șase miliarde de înregistrări în 30 de zile. Barele deschise la culoare sunt înregistrări de „DNR“ (apeluri telefonice), iar cele închise la culoare sunt „DNI“ (activitate pe internet):



Pentru a strânge aceste miliarde de înregistrări telefonice, SSO colaborează cu parteneri corporativi ai NSA, precum și cu agenţii guvernamentale străine – de exemplu, serviciul de informaţii polonez:

> (TS//SI//NF) ORANGECRUSH, parte a programului OAKSTAR sub portofoliul corporativ al SSO, a început să trimită metadate de la un partener terţ (Polonia) către sistemele de stocare ale NSA din 3 martie, iar conţinut din 25 martie. Acest program este un efort de colaborare între SSO, NSCS, ETC, FAD, un Partener Corporativ al NSA şi o divizie a guvernului polonez. ORANGECRUSH este cunoscut polonezilor ca BUFFALOGREEN. Acest parteneriat multiplu a început în mai 2009 şi va încorpora proiectul OAKSTAR al ORANGEBLOSSOM şi capacităţile sale DNR. Noul acces va oferi SIGINT prin legături comerciale gestionate de Partenerul Corporativ al NSA şi se anticipează că va include comunicaţiile Armatei Naţionale Afghane, cele din Orientul Mijlociu, o parte din cele de pe continentul african şi cele europene. O notificare a fost postată pe SPRINGRAY şi această colectare este disponibilă pentru Partenerii Secundari prin TICKETWINDOW.

Programul OAKSTAR exploatează în mod similar accesul pe care unul dintre partenerii corporativi ai NSA (cu numele de cod STEELKNIGHT) îl are la sistemele de telecomunicaţii

străine, folosind acest acces pentru redirecţionarea datelor către sistemele de stocare ale NSA. Un alt partener, cu numele de cod SILVERZEPHYR, apare într-un document din 11 noiembrie 2009 care descrie activitatea efectuată în colaborare cu compania pentru a obţine „comunicaţii interne“ din Brazilia și Columbia:

SILVERZEPHYR FAA DNI Acces Inițiat la NSAW (TS//SI//NF)

De NUME REDACTAT la 2009-11-06 0918

(TS//SI//NF) În ziua de joi, 5/11/09, accesul SSO-OAKSTAR SILVERZEPHYR (SZ) a început să trimită înregistrări FAA DNI către NSAW via sistemul FAA WealthyCluster2/Tellurian instalat pe terenul partenerului. SSO a colaborat cu Biroul pentru Fluxul de Date și a trimis numeroase fișiere eșantion către o partiție test pentru validare, care au fost un succes complet. SSO va continua să monitorizeze fluxul și colectarea pentru a se asigura că orice anomalie este identificată și corectată în mod corespunzător. SILVERZEPHYR va continua să ofere clienților colectarea autorizată a tranzitului de DNR. SSO lucrează cu partenerii pentru a obține acces la alți 80 Gb de date DNI de pe rețeaua cu care este în peering, în pachete de 10 Gb. Echipa OAKSTAR, cu sprijin din partea NSAT și GNDA, tocmai a terminat un studiu SIGINT de 12 zile la fața locului, care a identificat peste 200 de noi legături. În timpul studiului, GNDA a colaborat cu partenerul pentru a testa capacitatea sistemului lor ACS. OAKSTAR lucrează, de asemenea, cu NSAT pentru a examina instantaneele realizate de parteneri în Brazilia și Columbia, iar ambele pot conține comunicații interne pentru aceste țări.

Un alt program, STORMBREW, realizat „în strâns parteneriat cu FBI“, oferă NSA acces la traficul de internet și telefonie care intră în Statele Unite prin diverse „puncte cu trafic intens“ de pe teritoriul SUA. Acesta exploatează faptul că majoritatea traficului pe internet din lume la un moment dat trece prin infrastructura de comunicaţii a SUA – un subprodus rezidual al rolului central pe care Statele Unite l-au jucat în dezvoltarea reţelei. Unele dintre aceste puncte cu trafic intens menţionate sunt identificate prin nume de cod:

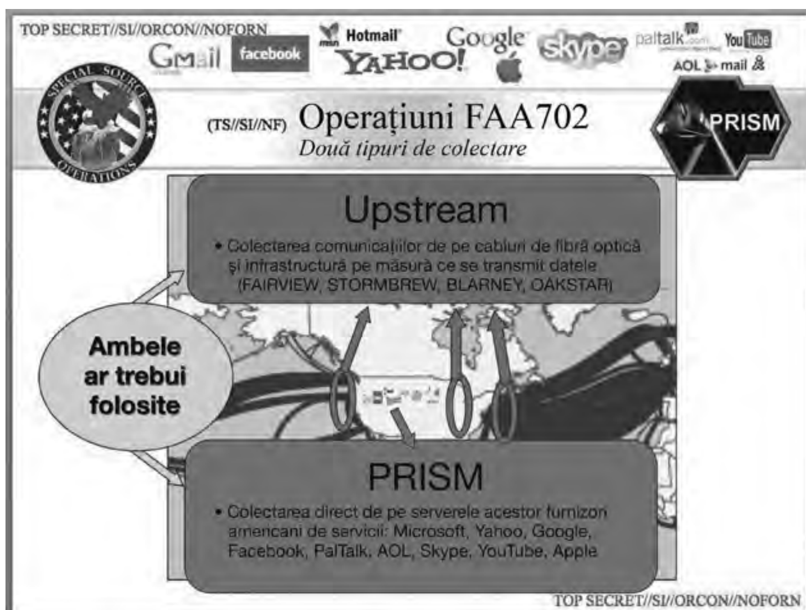


Potrivit NSA, STORMBREW „reprezintă în prezent relaţia foarte sensibilă cu doi furnizori de telecomunicaţii (cu numele de cod ARTIFICE și WOLFPOINT)“. Dincolo de accesul său la punctele de trafic intens de pe teritoriul SUA, „programul STORMBREW gestionează și două puncte de convergenţă a cablurilor submarine, unul pe coasta de vest a SUA (denumit BRECKENRIDGE), celălalt pe coasta de est (denumit QUAILCREEK)“.

Așa cum demonstrează abundența numelor de cod, identitatea partenerilor săi corporativi este unul dintre cele mai bine păstrate secrete în NSA. Documentele care conţin cheia acestor nume de cod sunt păzite vigilent de agenţie și Snowden nu a putut obţine multe dintre ele. În orice caz, dezvăluirile lui au demascat unele dintre companiile care cooperează cu NSA. Cel mai cunoscut exemplu îl reprezintă documentele PRISM, care detaliază acorduri secrete între NSA și cele mai mari companii de internet din lume – Facebook, Yahoo!, Apple, Google –,

precum și eforturile vaste ale Microsoft de a furniza agenţiei acces la platformele sale de comunicare precum Outlook.

Spre deosebire de programele BLARNEY, FAIRVIEW, OAKSTAR și STORMBREW, care presupun interceptarea cablurilor de fibră optică și a altor forme de infrastructură (supraveghere „upstream", în limbaj NSA), PRISM permite NSA să colecteze date direct de pe serverele a nouă dintre cele mai mari companii de internet:



Companiile listate în slide-ul PRISM neagă că au permis NSA acces nelimitat la serverele lor. Facebook și Google, de exemplu, pretind că oferă NSA doar informaţii pentru care agenţia are mandat și încearcă să descrie PRISM ca fiind ceva mai mult decât un detaliu tehnic neînsemnat: un sistem de livrare ușor modernizat prin care NSA primește date într-o „lockbox", date pe care companiile sunt obligate legal să le furnizeze.

Dar argumentul lor este contrazis de numeroase date. În primul rând, știm că Yahoo! luptă acerb în justiţie împotriva eforturilor NSA de a o forţa să se alăture PRISM – un efort improbabil dacă programul ar fi fost o simplă schimbare neînsemnată a sistemului de livrare. (Acţiunea Yahoo! a fost respinsă de tribunalul FISA, iar companiei i s-a ordonat să participe la PRISM.) În al doilea rând, Bart Gellman de la *Washington Post*, după ce a fost aspru criticat[9] că a exagerat impactul PRISM, a reinvestigat programul și a confirmat că menţine principala afirmaţie a *The Post*: „Din sediile lor de oriunde în lume, angajaţii guvernamentali care au primit acces la PRISM pot «pune la treabă» sistemul – adică pot demara o căutare – și primi rezultate de la o companie de internet fără o interacţiune ulterioară cu personalul companiei".

În al treilea rând, negările companiilor de internet au fost exprimate într-un mod evaziv și în litera legii, adeseori mai mult încurcând decât clarificând lucrurile. De exemplu, Facebook a pretins că nu oferă „acces direct", în timp ce Google a negat că a creat un „backdoor"* pentru NSA. Dar așa cum a declarat Chris Soghoian, expertul tehnic al ACLU,pentru *Foreign Policy*[10], aceștia sunt termeni foarte tehnici care denumesc mijloace foarte specifice de obţinere a informaţiei. În cele din urmă, companiile nu au negat că au colaborat cu NSA pentru a înfiinţa un sistem prin care agenţia poate accesa direct datele clienţilor lor.

În final, NSA a lăudat în mod repetat PRISM pentru capacităţile sale unice de colectare și a menţionat că programul a fost vital pentru creșterea supravegherii. Un slide NSA detaliază puterile speciale de supraveghere ale PRISM:

* Cale secretă utilizată pentru a obţine acces în cadrul unui software sau serviciu online (n.tr.)

TOP SECRET//SI//ORCON//NOFORN

GMail facebook Hotmail YAHOO! Google skype paltalk YouTube AOL mail

(TS//SI//NF) Operațiuni FAA702

Folosirea ambelor: PRISM vs. Upstream

	PRISM	Upstream
Selectori DNI	✓ 9 furnizori de servicii cu sediul în SUA	✓ Surse din întreaga lume
Selectori DNR	⃠ Urmează în curând	✓ Surse din întreaga lume
Acces la comunicații stocate (căutare)	✓	⃠
Colectare în timp real (supraveghere)	✓	✓
Colectare „Despre"	⃠	✓
Colectare voce	✓ Voice over IP	✓
Relații directe cu furnizorii de comunicații	⃠ Doar prin FBI	✓

TOP SECRET//SI//ORCON//NOFORN

Un altul detaliază gama largă de comunicaţii la care NSA are acces prin intermediul PRISM:

TOP SECRET//SI//ORCON//NOFORN

GMail facebook Hotmail YAHOO! Google skype paltalk YouTube AOL mail

(TS//SI//NF) Detalii privind colectarea PRISM

Furnizori actuali

- Microsoft (Hotmail etc.)
- Google
- Yahoo!
- Facebook
- PalTalk
- YouTube
- Skype
- AOL
- Apple

Ce veți primi în timpul colectării (supraveghere și comunicații stocate)? Variază în funcție de furnizor. În general:

- E-mail
- Chat – video, voce
- Video
- Fotografii
- Date stocate
- VoIP
- Transfer de fișiere
- Videoconferințe
- Notificări privind activitatea țintei – autentificare etc.
- Detalii ale activității pe rețelele de socializare online
- **Solicitări Speciale**

Lista completă și detaliile pe pagina web a PRISM: Mergi la PRISMFAA

TOP SECRET//SI//ORCON//NOFORN

Un alt slide al NSA detaliază cum a sporit în mod constant și substanțial programul PRISM activitatea de colectare a agenției:



Pe platforma sa de mesagerie internă, diviziunea Operațiuni cu Sursă Specială [SSO] laudă în mod frecvent importanța colectării masive pe care a oferit-o PRISM. Un mesaj din 19 noiembrie 2012 este intitulat „Impactul expansiunii PRISM: Valorile anului fiscal 2012“:

(TS//SI//NF) PRISM (US-984XN) şi-a extins impactul asupra misiunii de raportare a NSA în anul fiscal 2012 prin creşterea numărului de sarcini, îmbunătăţirea activităţilor de colectare şi operaţionale. Iată câteva trăsături ale programului PRISM din anul fiscal 2012:

PRISM este cea mai citată sursă de colectare în raportările NSA de produse finale primare. Tot mai multe raportări de produse se bazează pe PRISM mai mult decât pe orice alt SIGAD pentru toate raportările primare ale NSA din anul fiscal 2012: citat în 15,1% din toate raportările (de la 14% în anul fiscal 2011). PRISM a fost citat în 13,4% din toate raportările NSA primare, secundare şi terţiare (de la 11,9% în anul fiscal 2011) şi este, de asemenea, cel mai citat SIGAD dintre toate.

Număr de raportări de produse finale bazate pe PRISM emise în anul fiscal 2012: 24 096, în creştere cu 27% începând cu anul fiscal 2011.

Proporție raportări dintr-o singură sursă în anii fiscali 2012 și 2011: 74%.

Număr de raportări de produse derivate din colectarea realizată de PRISM și citate ca surse în articole în informările zilnice ale președintelui (PDB) în anul fiscal 2012: 1477 (18% din toate raportările SIGINT citate ca surse în articolele PDB - cel mai ridicat SIGAD unic pentru NSA); în anul fiscal 2011: 1152 (15% din toate raportările SIGINT citate ca sursă în articolele PDB - cel mai mare SIGAD unic pentru NSA).

Număr de Elemente Esenţiale de Informaţie la care a contribuit în anul fiscal 2012: 4186 (32% din toate EEI pentru toate Necesităţile de Informaţie); 220 EEI adresate doar prin PRISM.

Atribuire de sarcini: Numărul selectorilor folosiţi a crescut cu 32% în anul fiscal 2012, la 45406 în septembrie 2012.

Mare succes în colectarea şi procesarea de pe Skype; ţinte unice, de mare valoare, atinse.

Domeniile de căutare în e-mailuri ale PRISM au fost extinse de la doar 40 la 22000.

Astfel de afirmaţii măgulitoare nu sprijină ideea că PRISM ar fi doar un detaliu tehnic fără însemnătate și dovedește falsitatea negărilor privind cooperarea din partea Silicon Valley. Într-adevăr, *New York Times*[11], relatând despre programul PRISM după dezvăluirile lui Snowden, a descris un număr mare de negocieri secrete între NSA și Silicon Valley în legătură cu oferirea unui acces nerestricţionat agenţiei la sistemele companiilor. „Când oficialii guvernamentali au venit la Silicon Valley pentru a cere modalităţi mai ușoare astfel încât cele mai mari companii de internet din lume să predea datele utilizatorilor lor în cadrul unui program de supraveghere secretă, companiile s-au înfuriat", a relatat *Times*. „Până la urmă însă multe au cooperat, chiar dacă unele într-o măsură mai mică." În special:

> Twitter a refuzat să facă acest lucru mai uşor pentru administrație. Dar alte companii au fost mai îngăduitoare, potrivit persoanelor informate în legătură cu negocierile. Ele au deschis discuțiile cu oficialii din domeniul securității naționale cu privire la dezvoltarea unor metode tehnice pentru a oferi acces mai eficient şi mai sigur la datele personale ale utilizatorilor străini ca răspuns la cererile legale ale administrației. Şi, în unele cazuri, au schimbat şi sistemele informatice pentru a face acest lucru.

Potrivit *New York Times*, aceste negocieri „ilustrează cât de strâns colaborează administraţia și companiile tehnologice și profunzimea tranzacţiilor lor din culise". Articolul contestă,

de asemenea, afirmaţiile companiilor că au furnizat NSA acces doar atunci când au fost obligate legal, notând: „În timp ce predarea datelor ca răspuns la o cerere legitimă a FISA este o solicitare legală, facilitarea obţinerii de informaţii de către administraţie nu este, de aceea Twitter a putut refuza să facă acest lucru“.

Afirmaţia companiilor de internet că au predat NSA doar informaţiile pe care erau obligate legal să le furnizeze nu este relevantă. Aceasta pentru că NSA are nevoie de mandat individual doar atunci când vrea să vizeze în mod specific o persoană din SUA. O astfel de permisiune nu este necesară pentru ca agenţia să obţină date din comunicaţiile altor cetăţeni decât cei americani de pe teritoriul străin, *chiar dacă persoana comunică cu americani*. În mod similar, nu există o verificare sau o limită pentru colectarea masivă de metadate a NSA, graţie interpretării oferite de administraţie a Patriot Act – o interpretare atât de extinsă, încât iniţiatorii legii au fost șocaţi să afle cum a fost folosită aceasta.

Colaborarea strânsă dintre NSA și corporaţiile private se poate vedea cel mai bine în documentele referitoare la Microsoft, care dezvăluie eforturile hotărâte ale companiei de a oferi NSA acces la câteva dintre cele mai folosite servicii online ale sale, inclusiv SkyDrive, Skype și Outlook.com.

SkyDrive, care permite persoanelor să stocheze fișiere online și să le acceseze de pe diverse dispozitive, are peste 250 de milioane de utilizatori în lume. „Noi credem că este important să aveţi control asupra a cine poate și cine nu să acceseze datele dumneavoastră personale din cloud“, proclamă website-ul SkyDrive al Microsoft. Așa cum detaliază documentele NSA, Microsoft a petrecut „multe luni“ lucrând pentru a oferi administraţiei un acces mai ușor la aceste date:

(TS//SI//NF) SSO IMPORTANT - Colectarea de la Microsoft Skydrive face acum parte din colectarea standard de comunicaţii stocate a PRISM

De NUME REDACTAT la 2013-03-08 1500

(TS//SI//NF) Începând cu 7 martie 2013, PRISM colectează date de la Microsoft Skydrive ca parte a pachetului standard de colectare a Comunicaţiilor Stocate pentru un selector vizat prin Secţiunea 702 a Legii FISA Amendate (FAA702). Aceasta înseamnă că analiştii nu vor mai trebui să prezinte o cerere specială SSO pentru acest lucru – o etapă a procesului despre care mulţi analişti este posibil să nu fi aflat. Această nouă capacitate va conduce la un răspuns mult mai complet şi mai oportun din partea SSO pentru companiile cliente. Acest succes este rezultatul colaborării timp de multe luni a FBI cu Microsoft pentru stabilirea acestor soluţii de alocare şi colectare. „SkyDrive este un serviciu cloud care le permite utilizatorilor să îşi stocheze şi să îşi acceseze fişierele de pe diverse dispozitive. Serviciul include, de asemenea, suport gratuit pentru aplicaţii web pentru programele Microsoft Office, astfel încât utilizatorul poate crea, edita şi vedea documente Word, PowerPoint, Excel fără să aibă de fapt instalat MS Office pe dispozitivul folosit.“ (sursa: S314 wiki)

La sfârșitul lui 2011, Microsoft a cumpărat Skype, serviciul de telefonie și chat prin internet cu peste 663 de milioane de utilizatori înregistraţi. La momentul cumpărării, Microsoft asigura utilizatorii că „Skype se angajează să respecte intimitatea și confidenţialitatea datelor dumneavoastră personale, traficului și conţinutului comunicaţiilor“. Dar în realitate, și aceste date au fost puse prompt la dispoziţia administraţiei. La începutul lui 2013, au fost multiple mesaje pe sistemul NSA care celebrau accesul, îmbunătăţit constant, al agenţiei la comunicaţiile utilizatorilor Skype:

(TS//SI//NF) Capacitate a noilor comunicaţii stocate ale Skype pentru PRISM

De NUME REDACTAT la 2013-04-03 0631

(TS//SI//NF) PRISM are o nouă capacitate de colectare: comunicaţiile stocate ale Skype. Comunicaţiile stocate ale Skype vor conţine date unice care nu sunt colectate în mod normal în cadrul activităţii de colectare prin supraveghere în timp real. SSO se aşteaptă să primească liste de prieteni, informaţii privind carduri de credit, înregistrări ale apelurilor, informaţii despre conturile utilizatorilor şi alte materiale. La 29 martie 2013, SSO a trimis aproximativ 2 000 de selectori Skype pentru comunicaţiile stocate în privinţa cărora să se ia o decizie în SV41 şi Unitatea de Supraveghere a Comunicaţiilor Electronice (ECSU) a FBI. SV41 a decis să aloce prioritate maximă selectorilor şi aproximativ 100 sunt gata pentru a fi evaluaţi de ECSU. Ar putea dura câteva săptămâni pentru ca SV41 să îi analizeze pe toţi cei 2 000 de selectori pentru a obţine aprobarea lor, iar ECSU va avea probabil nevoie de mai mult timp pentru a acorda aceste aprobări. Până la 2 aprilie, ECSU a aprobat peste 30 de selectori care să fie trimişi către Skype pentru colectare. Colectarea PRISM de la Skype a creat o nişă vitală în raportarea NSA în mai puţin de doi ani, cu rapoarte despre terorism, opoziţia şi regimul din Siria printre subiectele cele mai importante. Peste 2 800 de rapoarte au fost emise din aprilie 2011 pe baza colectării PRISM de la Skype, cu 76% dintre ele din sursă unică.

(TS//SI//NF) SSO extinde capacitatea PRISM de urmărire în cazul Skype

De NUME REDACTAT la 2013-04-03 0629

(TS//SI//NF) La 15 martie 2013, programul PRISM al SSO a început să aloce către Skype toţi selectorii PRISM pentru Microsoft pentru că Skype le permite utilizatorilor să se autentifice folosind identificatori pe lângă numele de utilizator Skype. Până în prezent, PRISM nu colecta nici o dată Skype atunci când un utilizator se conecta folosind orice altceva decât numele de utilizator Skype, ceea ce conducea la o pierdere de date; această acţiune va micşora pierderea. În fapt, un utilizator poate crea un cont Skype folosind orice adresă de e-mail pe orice domeniu din lume. UTT nu permite în prezent analiştilor să demareze căutări pentru aceste adrese de e-mail care nu aparţin Microsoft adresate PRISM, totuşi, SSO intenţionează să rezolve această problemă în vară. Între timp, NSA, FBI şi Departamentul de Justiţie s-au coordonat în ultimele şase luni pentru a obţine aprobarea pentru ca PRINTAURA să trimită toţi selectorii PRISM actuali şi viitori pentru Microsoft către Skype. Rezultatul a fost trimiterea a aproximativ 9000 de selectori către Skype şi s-a obţinut o colectare de succes, care altfel ar fi lipsit.

Nu numai că această colaborare a avut loc într-o totală lipsă de transparenţă, ci ea a contrazis declaraţiile publice făcute de Skype. Expertul în tehnologie al ACLU, Chris Soghoian, a declarat că dezvăluirile vor surprinde mulţi clienţi Skype.[12] „În trecut, Skype le-a făcut promisiuni utilizatorilor săi că nu vor fi interceptaţi“, a spus el. „Este greu să împaci colaborarea secretă a Microsoft cu NSA cu eforturile sale intense de a concura cu Google în privinţa intimităţii.“

În 2012, Microsoft a început să modernizeze portalul său de e-mail, Outlook.com, pentru a aduna la un loc toate serviciile sale de comunicaţii – inclusiv mult folositul Hotmail – într-un program central. Compania a lăudat noul Outlook promiţând niveluri ridicate de criptare pentru protejarea intimităţii, iar NSA a devenit rapid îngrijorată că această criptare oferită de Microsoft clienţilor Outlook va împiedica agenţia să le spioneze comunicaţiile. O notă SSO din 22 august 2012 manifestă îngrijorare cu privire la faptul că „folosirea acestui portal înseamnă că e-mailurile provenind de la el vor fi criptate prin setările implicite“ și că „sesiunile de chat desfășurate în cadrul portalului sunt, de asemenea, criptate când ambii utilizatori folosesc un client de chat criptat al Microsoft“.

Dar această îngrijorare a fost una de scurtă durată. În câteva luni, cele două entităţi s-au reunit și au elaborat metode pentru ca NSA să evite protecţiile criptate pe care Microsoft le prezentase public ca fiind vitale pentru protejarea intimităţii:

(TS//SI//NF) Microsoft inaugurează un nou serviciu care afectează colectarea pentru FAA 702

De NUME REDACTAT la 2012-12-26 0811

(TS//SI//NF) La 31 iulie, Microsoft (MS) a început să cripteze discuţiile online cu introducerea noului serviciu outlook.com. Această nouă metodă de criptare Secure Socket Layer (SSL) împiedică efectiv colectarea de noi servicii pentru FAA 702 şi probabil 12333 (într-o oarecare măsură) pentru Comunitatea de Informaţii (IC). MS a colaborat cu FBI şi a dezvoltat o capacitate de supraveghere care să facă faţă noului SSL. Aceste soluţii au fost testate cu succes şi au demarat la 12 decembrie 2012. Soluţia SSL a fost aplicată tuturor solicitărilor actuale FISA şi 702/PRISM – nu a fost cerută nici o schimbare pentru procedurile de căutare UTT. Soluţia SSL nu colectează voce/video de pe servere sau transferuri de fişiere. Sistemul de colectare existent al MS va rămâne în funcţiune pentru a colecta voce/video şi transferuri de fişiere. Ca urmare, vor fi unele duplicate ale discuţiilor text de la noul şi vechiul sistem care vor fi tratate la o dată ulterioară. O creştere a volumului de colectare ca urmare a acestei soluţii a fost deja remarcată de CES.

Un alt document descrie colaborarea ulterioară dintre Microsoft și FBI, în timp ce agenţia încerca să se asigure că noile caracteristici ale Outlook nu vor interfera cu obiceiurile sale de supraveghere: „Echipa pentru Tehnologia Interceptării Datelor (DITU) a FBI colaborează cu Microsoft ca să înţeleagă o caracteristică adiţională în Outlook.com care le permite utilizatorilor să creeze aliasuri de e-mail, care pot afecta procesul nostru de căutare... Există compartimentări și alte activităţi în desfășurare pentru a reduce aceste probleme".

Găsirea acestei menţiuni cu privire la supravegherea FBI în arhiva lui Snowden de documente interne ale NSA nu a fost un incident izolat. Întreaga comunitate de informaţii este capabilă să acceseze informaţiile pe care le colectează NSA; aceasta oferă acces de rutină la vasta sa comoară de date altor agenţii, inclusiv FBI și CIA. Unul dintre scopurile principale ale colectării de date a NSA a fost tocmai creșterea răspândirii informaţiei în cadrul comunităţii. Într-adevăr, aproape fiecare document aparţinând diverselor programe

de colectare menţionează includerea altor unităţi ale serviciilor de informaţii. Acest mesaj din 2012 de la unitatea SSO a NSA, cu privire la partajarea datelor PRISM, declară exuberant că „PRISM este un sport de echipă!“:

(TS//SI//NF) Extindere a partajării PRISM cu FBI şi CIA

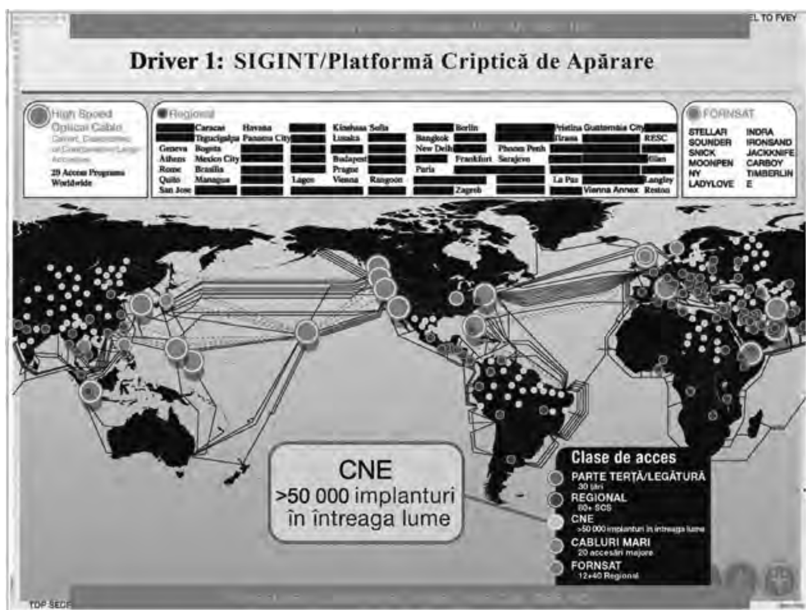
De NUME REDACTAT la 2012-08-31 0947

(TS//SI//NF) Operaţiuni cu Sursă Specială (SSO) a extins recent partajarea cu Biroul Federal de Investigaţii (FBI) şi Agenţia Centrală de Informaţii (CIA) în privinţa operaţiunilor PRISM prin două proiecte. Prin aceste eforturi, SSO a creat un mediu de partajare şi colaborare în cadrul Comunităţii de Informaţii pe operaţiuni PRISM. În primul rând echipa PRINTAURA a SSO a rezolvat o problemă pentru Signals Intelligence Directorate (SID), scriind un program care va strânge automat o listă a selectorilor de căutare PRISM la fiecare două săptămâni, pentru a o oferi FBI şi CIA. Aceasta le permite partenerilor noştri să vadă ce selectori a folosit Agenţia de Securitate Naţională (NSA) pentru PRISM. FBI şi CIA pot cere apoi o copie a colectării PRISM pentru orice selector, aşa cum permit amendamentele la Legea privind supravegherea activităţilor străine de spionaj (FISA) din 2008. Înainte de activitatea PRINTAURA, SID a oferit FBI şi CIA liste incomplete şi inexacte, împiedicându-i pe partenerii noştri să se folosească pe deplin de programul PRISM. PRINTAURA s-a oferit în mod voluntar să strângă date detaliate legate de fiecare selector din mai multe locuri şi să le reunească sub o formă ce poate fi folosită. În al doilea proiect, Managerul de Program al Misiunii (MPM) PRISM a început recent să trimită informaţii operaţionale PRISM şi îndrumări FBI şi CIA pentru ca analiştii lor să poată folosi sistemul PRISM în mod corespunzător, să fie avertizaţi de întreruperi şi schimbări şi să optimizeze folosirea PRISM. MPM a coordonat un acord din partea echipei SID FAA (Legea amendată privind supravegherea activităţilor străine de spionaj) pentru a partaja aceste informaţii săptămânal, iniţiativă bine primită şi apreciată. Aceste două activităţi subliniază faptul că PRISM este un sport de echipă!

Colectarea „Upstream“ (din cabluri de fibră optică) și colectarea directă de la serverele companiilor de internet (PRISM) sunt responsabile de cele mai multe înregistrări strânse de NSA. În plus faţă de această supraveghere extinsă, NSA desfășoară și ceea ce numește Computer Network Exploitation (CNE) [Exploatarea Reţelei de Calculatoare], amplasând programe malware în computere individuale pentru a supraveghea utilizatorii. Când agenţia reușește să insereze astfel de programe malware, ea este capabilă, în terminologia NSA, să „deţină“ computerul: pentru a vizualiza fiecare tastare și fiecare ecran vizualizat. Divizia Tailored Access Operations (TAO)

[Operaţiuni de Acces la Comandă] responsabilă de această activitate este, de fapt, unitatea privată de hackeri a agenţiei.

Practica piratării calculatoarelor este, la rândul ei, destul de răspândită: un document NSA arată că agenţia a reușit să infecteze cel puţin 50 000 de computere individuale cu un tip de malware denumit „Quantum Insertion“. O hartă arată locurile unde a fost desfășurată această operaţiune și numărul inserărilor reușite:



Folosind documentele lui Snowden, *New York Times* a relatat că NSA a implantat de fapt acest program „în aproximativ 100 000 de computere din întreaga lume“.[13] Deși malware-ul este de obicei instalat prin „obţinerea accesului la reţeaua de calculatoare, NSA a folosit tot mai mult o tehnologie secretă care îi permite să intre și să modifice datele din computere chiar dacă acestea nu sunt conectate la internet“.

Dincolo de activitatea sa cu firmele de telecomunicaţii și internet docile, NSA a colaborat și cu guverne străine pentru a-și construi sistemul de supraveghere de mare anvergură. În general, NSA are trei categorii diferite de relaţii externe. Prima este cu grupul Five Eyes: SUA spionează împreună cu aceste ţări, dar rareori le spionează pe ele, cu excepţia unei solicitări în acest sens a oficialilor acestor ţări. Al doilea nivel implică ţări cu care NSA lucrează pe proiecte specifice de supraveghere în timp ce le spionează pe larg. Al treilea grup este format din ţări pe care Statele Unite le spionează de rutină, dar cu care practic nu cooperează niciodată.

În cadrul grupului Five Eyes, cel mai apropiat aliat este agenţia britanică GCHQ. Așa cum a relatat *Guardian*[14], pe baza unor documente oferite de Snowden, „administraţia americană a plătit cel puţin 100 de milioane de lire sterline agenţiei de spionaj britanice GCHQ în ultimii trei ani pentru a-și asigura accesul și pentru a influenţa programele de strângere de informaţii ale Marii Britanii". Aceste plăţi reprezentau un stimulent ca GCHQ să sprijine agenda de supraveghere a NSA. „GCHQ trebuie să muncească la fel de mult și să fie văzută ca muncind la fel de mult", susţine o notă secretă privind strategia GCHQ.

Membrii Five Eyes partajează cea mai mare parte a activităţilor lor de supraveghere și se întâlnesc în fiecare an la o conferinţă privind evoluţia interceptării semnalelor, unde se laudă cu extinderea lor și succesele anului precedent. Fostul director adjunct al NSA, John Inglis, a declarat despre alianţa Five Eyes că „practică activitatea de *intelligence* în multe privinţe în mod combinat – în principal asigurându-ne că ne exploatăm unii altora capacităţile pentru un beneficiu mutual".

Multe dintre programele de supraveghere cele mai invazive sunt desfășurate de partenerii Five Eyes, un număr substanţial al acestora implicând GCHQ. De remarcat sunt eforturile comune ale agenţiei britanice și NSA de a sparge tehnicile de criptare comună folosite pentru protejarea tranzacţiilor personale pe internet, cum ar fi activitatea bancară online

și recuperarea datelor medicale. Succesul celor două agenţii în instalarea unor backdoors pentru a accesa aceste sisteme criptate nu numai că le-a permis să cerceteze activităţile private ale persoanelor, ci a și slăbit sistemele pentru toţi, făcându-le mai vulnerabile la hackeri rău intenţionaţi sau la alte agenţii de spionaj străine.

GCHQ a desfășurat, de asemenea, activităţi de interceptare masivă a datelor de comunicaţii din cablurile de fibră optică subterane din lume. Prin programul denumit Tempora, GCHQ a dezvoltat „abilitatea de a intercepta și stoca volume uriașe de date extrase din cablurile de fibră optică până la 30 de zile, astfel încât să fie examinate și analizate“[15], a relatat *Guardian*, iar „GCHQ și NSA sunt, prin urmare, capabile să acceseze și să proceseze cantităţi vaste de comunicaţii între persoane complet nevinovate“. Datele interceptate cuprind toate formele de activitate online, inclusiv „înregistrări de apeluri telefonice, conţinutul mesajelor electronice, intrări pe Facebook și istoricul accesărilor de website-uri ale utilizatorilor de internet“.

Activităţile de supraveghere ale GCHQ sunt la fel de cuprinzătoare – și nenumărate – ca și cele ale NSA. *Guardian* a menţionat:

> Măsura ambiției agenției se reflectă în denumirile celor două principale componente ale sale – Controlarea Internetului şi Exploatarea Rețelei Globale de Telecomunicații –, menite să adune cât de mult trafic online şi telefonic se poate. Toate acestea au loc fără vreun fel de recunoaștere sau de dezbatere publică.

Canada este, de asemenea, un partener foarte activ al NSA și ea însăși o forţă de supraveghere în domeniul energetic. La conferinţa SigDev din 2012, Centrul pentru Securitatea Telecomunicaţiilor Canada (CSEC) s-a lăudat că a urmărit Ministerul Minelor și Energiei din Brazilia, agenţia care reglementează industria de mare interes pentru companiile canadiene:

ȘI LE-AU SPUS TITANILOR: „PĂZIȚI-VĂ, AU VENIT OLIMPIENII!“

CSEC – Rețeaua avansată a metodologiei informativ-operative (tradecraft)

Conferința SD din iunie 2012

Overall Classification: TOP SECRET//SI

OLYMPIA & STUDIUL DE CAZ

OLYMPIA

Motorul de informații al rețelei CSEC

Șurse de date variate
Îmbunătățiri în serie
Analiză automată

Ministerul Minelor și Energiei (MME) din Brazilia

De dezvoltat noua țintă
Acces limitat/cunoaștere a țintei

TOP SECRET // SI

Există dovezi cu privire la cooperarea extinsă CSEC/NSA, inclusiv eforturile Canadei de a înfiinţa posturi de spionaj pentru supravegherea comunicaţiilor în toată lumea în numele și în beneficiul NSA și de a spiona parteneri comerciali vizaţi de agenţia americană.

STRICT SECRET//SI//REL USA, FVEY



Agenţia de Securitate Naţională/ Serviciul de Securitate Central

3 aprilie 2013

Document de informare

Subiect: (U//FOUO) Relația NSA cu Centrul pentru Securitatea Comunicațiilor Canada (CSEC)

STRICT SECRET//SI//REL TO SUA, CAN

(U) Ce furnizează NSA partenerului:

3 aprilie 2013

(SI//SI//REL TO USA, CAN) SIGINT: NSA şi CSEC cooperează în urmărirea a aproximativ 20 de ţări cu prioritate ridicată. [redacted] NSA partajează progres tehnologic, capacităţi criptologice, software şi resurse pentru colectarea la cel mai înalt nivel, eforturi de procesare şi analiză şi capacităţi IA. Schimbul de informaţii cu CSEC acoperă ţinte naţionale şi transnaţionale din toată lumea. Nu sunt alocaţi bani prin Programul Criptologic Unificat (CCP) către CSEC, dar NSA plăteşte uneori costurile pentru R&D (cercetare şi dezvoltare) şi tehnologice ale proiectelor comune cu CSEC.

(U) Ce furnizează partenerul NSA:

(TS//SI//REL TO USA, CAN) CESC oferă resurse pentru colectare, procesare şi analiză avansate şi a deschis site-uri sub acoperire la cererea NSA. CSEC partajează cu NSA accesul geografic unic la zonele indisponibile SUA [redacted] şi oferă produse criptografice, analiză criptografică, tehnologie şi software. CSEC a crescut investiţiile în proiecte R&D de interes comun.

Relaţia între partenerii Five Eyes este atât de strânsă, încât guvernele membre pun dorinţa NSA înaintea dreptului la viaţă privată al propriilor cetăţeni. *Guardian* a relatat despre o notă din 2007[16], de exemplu, care descrie un acord „care a permis agenţiei să «demascheze» și să păstreze date personale despre britanici care nu putuseră fi accesate anterior“. În plus, regulile au fost schimbate în 2007 „pentru a permite NSA să analizeze și să reţină orice număr de mobil sau de fax, e-mailuri și adrese IP ale cetăţenilor britanici colectate de reţeaua sa“.

Mergând un pas mai departe, în 2011 guvernul australian a cerut explicit NSA să „extindă“ parteneriatul și să supună cetăţenii australieni unei supravegheri mai mari. Într-o scrisoare datată 21 februarie, directorul adjunct în exerciţiu al Defence Signals Directorate [Agenţia de Spionaj Electronic] din Australia scrie Signals Intelligence Directorate al NSA, pretinzând că Australia „se confruntă cu o ameninţare gravă și hotărâtă din partea unor extremiști «născuţi și crescuţi pe teritoriul său», activi atât în străinătate, cât și în Australia“. El a cerut creșterea supravegherii comunicaţiilor cetăţenilor australieni consideraţi suspecţi de guvernul lor:

> Deși am investit un efort analitic şi de colectare semnificativ pentru a găsi şi exploata aceste comunicații, dificultățile cu care ne confruntăm în obținerea unui acces regulat şi de încredere la aceste comunicații au impact asupra abilității noastre de a detecta şi preveni actele teroriste şi ne diminuează capacitatea de a proteja viețile şi siguranța cetățenilor australieni şi pe cele ale prietenilor şi aliaților noştri apropiați.
>
> Ne-am bucurat de un parteneriat îndelungat şi foarte productiv cu NSA în obținerea unui acces redus la colectarea garantată a SUA împotriva țintelor noastre teroriste de mare importanță în Indonezia. Acest acces a fost esențial pentru eforturile DSD de a distruge şi limita capacitățile operaționale ale teroriştilor în regiunea noastră, aşa cum a subliniat arestarea recentă a atacatorului fugar din Bali, Umar Patek.

> Am aprecia foarte mult oportunitatea de extindere a acestui parteneriat cu NSA, pentru a acoperi numărul tot mai mare de australieni implicați în activități extremiste internaționale – în particular australieni care au legături cu AQAP*.

Dincolo de partenerii din cadrul Five Eyes, următorul nivel de cooperare al NSA este în cadrul aliaţilor de Nivel B: ţările care au o cooperare limitată cu agenţia și sunt vizate ele însele de o supraveghere agresivă și nesolicitată. NSA a delimitat clar cele două niveluri de alianţă:

CONFIDENŢIAL//NOFORN//20291123

NIVEL A **Cooperare vastă**	Australia Canada Marea Britanie Noua Zeelandă
NIVEL B **Cooperare punctuală**	Austria Belgia Coreea de Sud Danemarca Elveţia Germania Grecia Islanda Italia Japonia Luxembourg Norvegia Olanda Polonia Portugalia Republica Cehă Spania Suedia Turcia Ungaria

* Al-Qaeda în Peninsula Arabă (n.tr.)

Folosind diferite denumiri (referindu-se la Nivelul B ca la Părţi Terţe), un document mai recent al NSA –„Recenzie a Partenerilor Străini“ din anul fiscal 2013 – arată o creștere a listei partenerilor NSA, prin includerea unor organizaţii internaţionale, precum NATO:

TOP SECRET// COMINT //REL USA, AUS, CAN, GBR, NZL

Parteneri SIGINT aprobați

Părți secunde

Australia
Canada
Marea Britanie
Noua Zeelandă

Coaliții

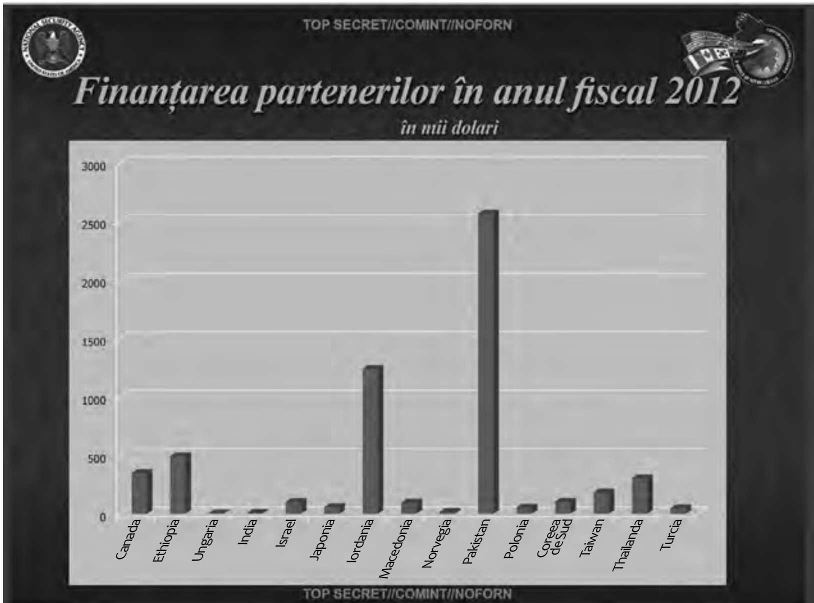
AFSC
NATO
SSEUR
SSPAC

Părți terțe

Algeria
Arabia Saudită
Austria
Belgia
Coreea de Sud
Croația
Danemarca
Emiratele Arabe Unite
Ethiopia
Finlanda
Franța
Germania
Grecia
India
Iordania
Israel
Italia
Japonia
Macedonia
Olanda
Norvegia
Pakistan
Polonia
Republica Cehă
România
Singapore
Spania
Suedia
Taiwan
Thailanda
Tunisia
Turcia

TOP SECRET// COMINT //REL USA, AUS, CAN, GBR, NZL

Ca și în cazul GCHQ, NSA menţine deseori aceste parteneriate plătindu-și partenerii pentru a dezvolta anumite tehnologii și pentru a se implica în supraveghere, și de aceea poate dicta cum să se desfășoare spionajul. „Recenzia Partenerilor Străini“ din anul fiscal 2012 dezvăluie că numeroase ţări au primit astfel de plăţi, inclusiv Canada, Israel, Japonia, Iordania, Pakistan, Taiwan și Thailanda:



În particular, NSA are o relaţie de supraveghere cu Israelul care implică deseori o cooperare la fel de strânsă ca parteneriatul Five Eyes, dacă nu și mai strânsă uneori. Un memorandum privind acordul între NSA și serviciul de informaţii israelian detaliază modul în care Statele Unite fac pași neobișnuiţi în partajarea de rutină cu Israelul a informaţiilor brute conţinând comunicaţii ale cetăţenilor americani. Printre datele furnizate Israelului sunt „transcrieri neverificate și integrale, idei, facsimile, telex, voce, metadate și conţinut din informaţiile obţinute prin interceptarea datelor electronice (Digital Network Intelligence – DNI)".

Ceea ce face această partajare extraordinară este că materialul e trimis Israelului fără să fi trecut prin procesul de „minimizare" necesar din punct de vedere legal. Procedurile de minimizare ar trebui să garanteze că, atunci când supravegherea masivă a NSA interceptează unele date a căror colectare nu este permisă nici măcar de cadrul foarte extins al agenţiei,

aceste informaţii vor fi distruse cât mai repede posibil și nu vor fi transmise mai departe. Așa cum este scrisă legea, cerinţele privind minimizarea au deja numeroase portiţe, inclusiv excepţii pentru „informaţii semnificative din activitatea de spionaj extern“ sau orice „dovadă a unei infracţiuni“. Dar atunci când este vorba despre transmiterea datelor serviciilor de informaţii israeliene, NSA pare să se fi dispensat de toate aceste aspecte legale.

Nota afirmă categoric: „NSA trimite de rutină ISNU (unităţii naţionale israeliene care se ocupă de SIGINT) colectări brute minimizate și neminimizate“.

Subliniind cum o ţară poate atât să coopereze în privinţa supravegherii, cât și să fie ţinta acesteia, documentul NSA, care reia istoria cooperării Israelului, remarcă „problemele de încredere care gravitează în jurul precedentelor operaţiuni ISR“ și identifică Israelul ca pe unul dintre cele mai agresive servicii de supraveghere care acţionează împotriva Statelor Unite:

> (TS//SI//REL) Există și câteva surprize... Franța vizează DoD al SUA prin colectări de informații tehnice, iar Israelul ne vizează de asemenea. Pe de o parte, israelienii sunt parteneri SIGINT extraordinar de buni pentru noi, dar pe de altă parte ne spionează pentru a afla pozițiile noastre în privința problemelor dinOrientul Mijlociu. O NIE (estimare a activității de spionaj și supraveghere la nivel național) îi plasează pe locul trei în rândul celor mai agresive servicii de informații care acționează împotriva SUA.

Același raport remarcă faptul că, în pofida relaţiei apropiate dintre agenţiile de spionaj americană și israeliană, informaţia vastă furnizată Israelului de Statele Unite nu determină un schimb la fel de productiv pentru SUA. Serviciile de informaţii israeliene sunt interesate doar de colectarea datelor care le ajută pe ele. Așa cum s-a plâns NSA, parteneriatul a fost ajustat „aproape total“ pentru nevoile Israelului.

Echilibrarea schimbului SIGINT între SUA și Israel a fost o provocare constantă în ultimul deceniu; acesta înclină fără îndoială puternic în favoarea preocupărilor de securitate ale Israelului. 11 septembrie a venit și s-a dus, iar singura relație reală de Parte Terță a NSA în privința contraterorismului este guvernată aproape total de nevoile partenerului.

O treaptă inferioară, sub partenerii din Five Eyes și ţările de nivel doi precum Israelul, nivelul trei este format din ţări care sunt deseori ţinte, dar niciodată parteneri ai SUA în programele de spionaj. Acest nivel include, în mod predictibil, guverne văzute drept adversare, precum China, Rusia, Iran, Venezuela și Siria. Dar nivelul trei include și ţări considerate, în general, prietenoase sau neutre, precum Brazilia, Mexic, Argentina, Indonezia, Kenya și Africa de Sud.

Când au apărut dezvăluirile despre NSA, administraţia SUA a încercat să își apere acţiunile afirmând că, spre deosebire de cetăţenii străini, cei americani sunt protejaţi de supravegherea NSA fără mandat. La 18 iunie 2013, președintele Obama i-a declarat lui Charlie Rose[17]: „Ce pot spune fără echivoc este că, dacă ești cetăţean american, NSA nu îţi poate asculta telefonul... conform legii și reglementărilor, decât dacă... merge în faţa unui tribunal și obţine un mandat și caută o cauză probabilă, așa cum s-a întâmplat mereu“. Președintele republican al Comisiei pentru serviciile de informaţii din Camera Reprezentanţilor, Mike Rogers, a făcut o declaraţie similară pentru CNN[18], susţinând că NSA „nu ascultă telefoanele americanilor. Dacă face acest lucru, o face ilegal. Acest lucru încalcă legea“.

Aceasta a fost mai degrabă o linie stranie de apărare: de fapt, i se spune restului lumii că NSA încalcă viaţa privată a celor care nu sunt americani. Protecţia intimităţii pare să fie doar pentru cetăţenii americani. Mesajul a generat o atât de mare nemulţumire la nivel internaţional, încât chiar președintele Facebook, Mark Zuckerberg, nu tocmai un exemplu de

apărare a intimităţii, s-a plâns că administraţia SUA „l-a lovit“ prin răspunsul la scandalul NSA, punând în pericol interesele companiilor internaţionale de internet: „Administraţia a spus: Nu vă faceţi griji, nu spionăm nici un american. Minunat, este de mare ajutor pentru companiile care încearcă să lucreze cu oameni din lumea întreagă. Mulţumesc că aţi spus acest lucru și că aţi fost clari. Cred că a fost ceva foarte nepotrivit“.[19]

În afară de faptul că a fost o strategie ciudată, afirmaţia este în mod evident falsă. De fapt, contrar negărilor repetate ale președintelui Obama și ale oficialilor săi de rang înalt, NSA interceptează continuu comunicaţiile cetăţenilor americani, fără vreun mandat individual pentru o „cauză probabilă“ care să justifice o astfel de supraveghere. Aceasta pentru că legea FISA din 2008, așa cum am subliniat anterior, permite NSA – fără mandat individual – să monitorizeze conţinutul comunicaţiilor oricărui american, atât timp cât acestea sunt efectuate cu un cetăţean străin vizat. NSA etichetează această colectare drept „incidentală“, ca și cum ar fi un accident minor că agenţia spionează americani. Dar implicaţia este falsă. Așa cum explică Jameel Jaffer, directorul adjunct pe probleme legale al ACLU[20]:

> Administrația spune de multe ori că această supraveghere a comunicațiilor americanilor este „incidentală“, ceea ce sună ca şi cum supravegherea de către NSA a apelurilor telefonice americane şi a e-mailurilor este întâmplătoare şi, chiar şi din perspectiva administrației, regretabilă.
>
> Dar când oficialii administrației Bush au cerut Congresului aceste noi atribuții pentru supraveghere, ei au spus destul de explicit că, evident, cele care prezintă cel mai mare interes pentru ei sunt comunicațiile americanilor. Vezi, de exemplu, FISA pentru secolul XXI, audiere în fața Comisiei juridice a Senatului de la cel de-al 109-lea Congres (2006) (declarația lui Michael Hayden), că unele comunicații „cu un interlocutor din Statele Unite“ sunt cele „care sunt cele mai importante pentru noi“.

> Principalul scop al legii din 2008 a fost să facă posibilă colectarea de către administrație a comunicațiilor internaționale ale *americanilor* – şi să colecteze aceste comunicații fără vreo referință că vreuna dintre aceste părți face ceva ilegal. Şi mare parte din apărarea administrației are ca scop să ascundă acest fapt, care este unul crucial: administrația nu are nevoie să „urmărească" americanii pentru a colecta volume uriaşe de comunicații ale acestora.

Profesorul Jack Balkin de la Școala de Drept Yale a fost de acord[21] că legea FISA din 2008 i-a oferit efectiv președintelui autoritatea de a desfășura un program „similar ca efect cu programul de supraveghere fără mandat" care a fost implementat în secret de George W. Bush. „Aceste programe pot include în mod inevitabil multe apeluri telefonice care implică americani care nu au absolut nici o legătură cu terorismul sau al-Qaeda".

O altă discreditare a asigurărilor lui Obama o reprezintă postura servilă a tribunalului FISA, care aprobă aproape orice solicitare de supraveghere trimisă de NSA. Apărătorii NSA laudă frecvent activitatea tribunalului FISA ca o dovadă a faptului că agenţia este supervizată. Totuși, tribunalul a fost înfiinţat nu ca o verificare reală a puterilor administraţiei, ci ca o măsură cosmetică menită să ofere o aparenţă de reformă pentru a contracara nemulţumirea publicului în legătură cu abuzurile din domeniul supravegherii dezvăluite în anii 1970.

Inutilitatea acestei instituţii ca modalitate reală de control a abuzurilor este evidentă, deoarece tribunalul FISA nu are practic nici un atribut din ceea ce societatea înţelege, în general, ca fiind elemente minime ale sistemului judiciar. Acesta se întrunește în cel mai mare secret; doar o singură parte – administraţia – poate participa la audieri și prezenta cazuri; iar deciziile tribunalului sunt automat desemnate strict secrete. La drept vorbind, ani la rând tribunalul FISA a fost găzduit de Departamentul de Justiţie, ceea ce arată clar apartenenţa sa la ramura executivă mai degrabă decât calitatea de organism judiciar independent care exercită o supervizare reală.

Rezultatele au fost cele așteptate: tribunalul nu a respins aproape niciodată cererile specifice ale NSA de a urmări americani. De la înfiinţarea sa, FISA a fost organismul final de autorizare automată. În primii săi 24 de ani de existenţă, din 1978 și până în 2002, tribunalul a respins în total *zero* solicitări ale administraţiei, în timp ce a aprobat câteva mii. În deceniul următor, până în 2012, tribunalul a respins doar 11 cereri. În total, acesta a aprobat peste 20 000 de cereri.

Una dintre prevederile legii FISA din 2008 cere ca ramura executivă să dezvăluie anual Congresului numărul de cereri de urmărire pe care curtea le primește și apoi le aprobă, modifică sau respinge. Dezvăluirea din 2012 arată că tribunalul a aprobat fiecare dintre cele 1 788 de cereri de supraveghere electronică pe care le-a analizat, în timp ce a „efectuat modificări“ – restrângând sfera ordinului – în doar 40 de cazuri, ceea ce reprezintă mai puţin de 3%.

Cereri adresate Curţii pentru supravegherea activităţii străine de spionaj în anul calendaristic 2012 (secţiunea 107 a legii, 50 U.S.C. § 1807)

În anul calendaristic 2012, administraţia a adresat 1 856 de cereri Curţii pentru supravegherea activităţii străine de spionaj (FISC) pentru a primi autorizaţia de a desfăşura supraveghere electronică şi/sau căutări fizice în scopul obţinerii de informaţii externe. Cele 1 856 de cereri includ solicitări făcute doar pentru supraveghere electronică, solicitări doar pentru percheziţii şi solicitări combinate care cer autorizaţie de supraveghere electronică şi percheziţii. Dintre acestea, 1 789 de cereri includ solicitări de supraveghere electronică.

Din cele 1 789 de cereri, una a fost retrasă de administraţie. FISC nu a respins nici o cerere integral sau parţial.

Aproape la fel s-a întâmplat și în 2011, când NSA a raportat 1 676 de cereri; tribunalul FISA a modificat 30 dintre ele, dar „nu a respins nici o cerere integral sau parţial“.

Servilismul tribunalului faţă de NSA este demonstrat și de alte statistici. Aici, de exemplu, este reacţia tribunalului FISA[22] în cei șase ani de diverse solicitări adresate de NSA în conformitate cu Patriot Act de a obţine date – telefonice, financiare

sau medicale – ale firmelor unor persoane care locuiesc legal pe teritoriul SUA:

Cereri de supraveghere adresate de administrație tribunalului FISA

An	Număr de solicitări privind înregistrările firmelor adresate de administrația SUA	Număr de solicitări respinse de tribunalul FISA
2005	155	0
2006	43	0
2007	17	0
2008	113	0
2009	21	0
2010	96	0
2011	205	0

[Sursa: Documente ale ODNI,18.11.2013]

Cu toate acestea, chiar și în cazurile limitate când este necesară aprobarea tribunalului FISA pentru supravegherea comunicaţiilor cuiva, procesul este mai mult o pantomimă decât o verificare, în adevăratul său sens, a NSA.

Un alt nivel al supervizării NSA este cel asigurat, de ochii lumii, de comisiile pentru serviciile de informaţii din Congres, create după scandalul privind supravegherea din anii 1970, dar acestea sunt și mai indolente decât tribunalul FISA. În timp ce ar trebui să desfășoare o „supraveghere legislativă vigilentă" a comunităţii de informaţii, aceste comisii sunt de fapt conduse în prezent de cele mai devotate persoane NSA din Washington: democrata Dianne Feinstein în Senat și republicanul Mike Rogers în Camera Reprezentanţilor. Mai degrabă decât să ofere o verificare critică a operaţiunilor NSA, comisiile conduse de Feinstein și Rogers există în primul rând pentru a justifica orice face agenţia.

Așa cum afirma Ryan Lizza în *New Yorker*, într-un articol din decembrie 2013, în loc să ofere o supraveghere, comisia Senatului de cele mai multe ori „tratează oficialii din cadrul serviciilor de informaţii ca pe niște staruri“.[23] Observatorii audierilor în comisii ale activităţilor NSA au fost șocaţi de modul în care era abordată audierea oficialilor NSA care apăreau în faţa lor. „Întrebările“ nu conţineau nimic mai mult decât niște monologuri lungi ale senatorilor legate de amintirile lor despre atacurile de la 11 septembrie și de cât de vitală este prevenirea unor astfel de atacuri pe viitor. Membrii comisiei au omis oportunitatea de a interoga acei oficiali și de a-și desfășura activitatea de supervizare, făcând în schimb propagandă în favoarea NSA. Scena surprinde perfect adevărata funcţie a comisiilor pentru serviciile de informaţii din ultimul deceniu.

Într-adevăr, președinţii comisiilor din Congres au apărat uneori NSA chiar și mai viguros decât înșiși oficialii agenţiei. La un moment dat, în august 2013, doi membri ai Congresului – democratul Alan Grayson din Florida și republicanul Morgan Griffith din Virginia – m-au abordat separat pentru a se plânge că încercările lor de a accesa cele mai elementare informaţii despre NSA sunt blocate de Comisia permanentă pentru serviciile de informaţii din Camera Reprezentanţilor. Amândoi mi-au dat scrisori pe care le scriseseră echipei președintelui Rogers în care cereau informaţii în legătură cu programele NSA despre care se discuta în presă. Cererile lor au fost respinse în mod repetat.

După articolele noastre despre Snowden, un grup de senatori din ambele partide, care erau de multă vreme îngrijoraţi în legătură cu abuzurile privind supravegherea, a început să elaboreze un proiect de lege care să impună limite reale puterilor NSA. Dar aceste reforme, conduse de senatorul democrat Ron Wyden din Oregon, au întâmpinat un blocaj imediat: eforturile desfășurate în contrapondere de apărătorii NSA în Senat de a redacta o legislaţie care să ofere doar o aparenţă de reformă,

în timp ce de fapt menţinea sau chiar creștea puterile NSA. Dave Weigel de la *Slate* relata în noiembrie[24]:

> Criticii colectării de date în masă de către NSA şi ai programelor de supraveghere nu au fost niciodată îngrijoraţi de lipsa de acţiune a Congresului. S-au aşteptat ca acesta să vină cu ceva care să pară o reformă, dar care de fapt a codificat şi a scuzat practicile dezvăluite şi criticate. Aşa se întâmplă întotdeauna – fiecare amendament sau reautorizare a Patriot Act din 2001 a construit mai multe portiţe decât ziduri.
>
> „Ne vom ridica împotriva unei brigăzi uzuale – formate din membri influenţi ai conducerii guvernamentale privind serviciile de informaţii, aliaţii lor din centrele de reflexie [sic] şi mediul academic, oficiali guvernamentali la pensie şi congresmeni care simpatizează cu ei“, a avertizat senatorul de Oregon Ron Wyden luna trecută. „Actul lor final asigură că orice reformă privind supravegherea este doar de suprafaţă... Normele de protecţie a intimităţii care nu protejează de fapt intimitatea nu valorează nici cât hârtia pe care sunt tipărite.“

Facţiunea privind „falsa reformă“ a fost condusă de Dianne Feinstein, acelaşi senator care exercita supervizarea primară a NSA. Feinstein a fost multă vreme loială industriei de securitate naţională a SUA, de la sprijinul ei vehement pentru războiul din Irak la sprijinul ferm pentru programele NSA din epoca Bush. (În acelaşi timp, soţul ei are participaţii majore în diverse contracte militare.) În mod clar, Feinstein a fost o alegere firească pentru a conduce o comisie care pretinde că supervizează comunitatea de informaţii, dar care de ani întregi a desfăşurat o funcţie opusă.

Prin urmare, cu toate negările administraţiei, NSA nu are limitări substanţiale în privinţa persoanelor pe care le poate spiona şi a modului de a face acest lucru. Chiar când astfel de limitări există în mod nominal – când cetăţenii americani sunt ţinta supravegherii –, procesul a devenit în mare măsură inutil. NSA este agenţia infractoare prin excelenţă, având puterea

de a face orice vrea cu foarte puţin control, transparenţă sau responsabilitate.

*

Foarte general vorbind, NSA colectează două tipuri de informaţii: conţinut și metadate. „Conţinutul“ se referă la ascultarea telefoanelor populaţiei sau citirea e-mailurilor ori a discuţiilor online, precum și la urmărirea activităţii pe internet, cum ar fi istoricul navigării sau activităţile de căutare. Colectarea „metadatelor“ implică strângerea de date despre aceste comunicaţii. NSA se referă la acestea drept „informaţii despre conţinut (dar nu conţinutul în sine)“.

Metadatele despre un mesaj electronic, de exemplu, înregistrează cine cui a trimis mesajul, când și de unde a trimis persoana respectivă mesajul. În ceea ce privește apelurile telefonice, informaţia include numerele de telefon ale apelantului și apelatului, cât timp au vorbit cei doi și deseori locul și tipul de dispozitiv folosit pentru a comunica. Într-un document despre apelurile telefonice, NSA a subliniat metadatele pe care le accesează și le stochează:

SECRET//COMINT//NOFORN//20320108

Câmpuri de metadate privind comunicarea în ICREACH

(S//NF) NSA completează următoarele câmpuri în PROTON

- Numere apelate și de la care s-a apelat, data, ora și durata apelului

(S//SI//REL) ICREACH vor vedea metadatele de telefonie în următoarele câmpuri:

DATE & TIME
DURATION – Length of Call
CALLED NUMBER
CALLING NUMBER
CALLED FAX (CSI) – Called Subscriber ID
TRANSMITTING FAX (TSI) – Transmitting Subscriber ID
IMSI – International Mobile Subscriber Identifier
TMSI – Temporary Mobile Subscriber Identifier
IMEI – International Mobile Equipment Identifier
MSISDN – Mobile Subscriber Integrated Services Digital Network
MDN – Mobile Dialed Number
CLI – Call Line Identifier (Caller ID)
DSME – Destination Short Message Entity
OSME – Originating Short Message Entity
VLR – Visitor Location Register

SECRET//COMINT//NOFORN//20320108

Administraţia SUA a insistat că mare parte din supravegherea dezvăluită în arhiva lui Snowden implică strângerea de „metadate, nu de conţinut", încercând să sugereze că acest tip de spionaj nu este intruziv – sau cel puţin nu la fel ca interceptarea conţinutului. Dianne Feinstein a afirmat explicit pentru *USA Today* că strângerea de metadate ale tuturor apelurilor telefonice ale americanilor „nu este supraveghere" deloc, pentru că „nu colectează conţinutul nici unei comunicaţii".

Aceste argumente nesincere ascund faptul că supravegherea metadatelor poate fi la fel de intruzivă ca și interceptarea conţinutului, iar uneori chiar mai intruzivă. Când administraţia știe orice persoană suni și oricine te sună pe tine, plus durata exactă a fiecărei conversaţii telefonice, când poate lista fiecare dintre persoanele cu care corespondezi pe e-mail și fiecare loc de unde ai trimis e-mailuri, poate crea o imagine remarcabilă despre viaţa ta, despre legăturile și activităţile tale, inclusiv unele dintre cele mai intime informaţii.

Într-un afidavit întocmit de ACLU[25] care contestă legalitatea programului NSA de colectare a metadatelor, profesorul de informatică și afaceri publice de la Princeton Edward Felten a explicat de ce supravegherea metadatelor poate fi revelatoare:

> Să luăm următorul exemplu ipotetic: o tânără îşi sună ginecologul; apoi îşi sună imediat mama; apoi un bărbat cu care a vorbit în mod repetat la telefon în ultimele luni după ora 23.00; după care sună la un centru de planificare familială care oferă şi posibilitatea de avort. Reiese o poveste probabilă care nu ar fi aşa de evidentă prin analizarea datelor unui singur apel telefonic.

Chiar și pentru un singur apel telefonic, metadatele pot oferi mai multe informaţii decât conţinutul apelului. Să asculţi telefonul unei femei care sună la o clinică de avorturi ar putea să nu dezvăluie nimic altceva decât că cineva confirmă o întâlnire cu o instituţie cu nume generic („East Side Clinic" sau „Dr. Jones's office"). Dar metadatele vor arăta mult mai mult decât

atât: vor dezvălui identitatea celor care au fost apelaţi. Același lucru este valabil și în cazul unui serviciu de întâlniri, al unui centru pentru gay și lesbiene, al unei clinici pentru dependenţii de droguri, al unui specialist HIV sau al unei linii telefonice de urgenţă pentru sinucigași. Metadatele vor demasca, de asemenea, o conversaţie între un activist pentru drepturile omului și un informator într-un regim opresiv sau o sursă confidenţială care sună un jurnalist pentru a dezvălui nereguli la nivel înalt. Și dacă suni în mod frecvent noaptea târziu pe cineva care nu îţi este soţ/soţie, metadatele vor dezvălui și acest lucru. Și mai mult, acestea vor înregistra nu numai cu cine și cât de des comunici, ci și toate persoanele cu care comunică prietenii și cunoscuții tăi, creând o imagine cuprinzătoare a reţelei tale de contacte.

Într-adevăr, așa cum remarcă profesorul Felten, supravegherea telefoanelor poate fi destul de dificilă din cauza diferenţelor de limbaj, a divagaţiilor, a folosirii argoului sau a codurilor deliberate și a altor atribute care fie intenţionat, fie accidental ascund înţelesul. „Conţinutul apelurilor telefonice este mult mai dificil de analizat în mod automat din cauza naturii sale nestructurate“, a argumentat el. Prin contrast, metadatele sunt matematice: curate, precise și ușor de analizat. Și, așa cum subliniază Felten, sunt deseori „un substitut pentru conţinut“:

> Metadatele telefonice pot... dezvălui extraordinar de multe informații despre obiceiurile şi asocierile noastre. Tiparele de apelare pot dezvălui când suntem treji sau când dormim; religia, dacă o persoană de obicei nu dă telefoane de sabat sau dă multe telefoane în ziua de Crăciun; obiceiurile şi aptitudinile sociale; numărul de prieteni şi chiar afilieri civile şi politice.

Pe scurt, scrie Felten, „colectarea în masă nu numai că permite administraţiei să afle informaţii despre mai multe persoane, ci îi permite să afle fapte noi care anterior erau private

și nu puteau fi aflate doar prin simpla colectare a informațiilor despre câțiva indivizi specifici".

Îngrijorarea în legătură cu numărul mare de utilizatori pe care administrația îi poate găsi prin acest tip sensibil de informații este justificată în special pentru că, spre deosebire de afirmațiile repetate ale președintelui Obama și NSA, este deja clar că numeroase activități ale agenției nu au nimic de-a face cu eforturile antiterorism sau chiar cu securitatea noastră națională. Mare parte din arhiva lui Snowden a dezvăluit ceea ce poate fi numit spionaj economic: supravegherea și interceptarea e-mailurilor îndreptate împotriva gigantului petrolier brazilian Petrobras, a conferințelor economice din America Latină, a companiilor energetice din Venezuela și Mexic și spionarea de către aliații NSA – inclusiv Canada, Norvegia și Suedia – a Ministerului Minelor și Energiei din Brazilia și a companiilor energetice din alte câteva țări.

Un document remarcabil prezentat de NSA și GCHQ detaliază numeroase ținte ale supravegherii care sunt în mod clar de natură economică: Petrobras, sistemul bancar SWIFT, compania petrolieră rusă Gazprom și cea aeriană rusă Aeroflot.

TOP SECRET//SI//REL TO USA, FVEY

Rețelele private sunt importante

- Multe ținte folosesc rețele private.

Infrastructura Google	Rețeaua SWIFT
REDACTAT	REDACTAT
REDACTAT	Gazprom
Aeroflot	REDACTAT
MFA Franța	REDACTAT
Warid Telecom	Petrobras
REDACTAT	REDACTAT

- Caracter evident în cercetare: 30–40% din traficul din BLACKPEARL are cel puțin o destinație finală privată.

TOP SECRET//SI//REL TO USA, FVEY

Ani la rând, președintele Obama și oficialii săi de rang înalt au denunţat vehement China pentru că își folosește capacităţile de supraveghere pentru a obţine avantaje economice, în timp ce insistau că Statele Unite și aliaţii lor nu fac niciodată acest lucru. *Washington Post* a citat un purtător de cuvânt al NSA care afirma că Departamentul Apărării, din care face parte agenţia, „este implicat în exploatarea reţelelor de computere“ dar „***nu*** în spionaj economic indiferent de domeniu, inclusiv «cibernetic»“[26] (asteriscuri ostentative în original].

Faptul că s-a negat că NSA spionează tocmai din motive economice este dovedit de propriile sale documente. Agenţia acţionează în beneficiul a ceea ce numește „clienţii“ săi, o listă care include nu numai Casa Albă, Departamentul de Stat și CIA, ci și agenţii în primul rând economice, precum Reprezentanţa SUA pentru Comerţ și Departamentele Agriculturii, Trezoreriei și Comerţului:



În descrierea programului BLARNEY, NSA enumeră tipurile de informaţii pe care trebuie să le furnizeze clienţilor săi, precum „contraspionaj“, „diplomatice“ – și „economice“:

TOP SECRET // COMINT // NOFORN//20291130

BLARNEY DINTR-O PRIVIRE

De ce: Inițiat în 1978 cu scopul de a furniza FISA acces la comunicațiile instituțiilor străine, ale agenților unor puteri străine și ale teroriștilor

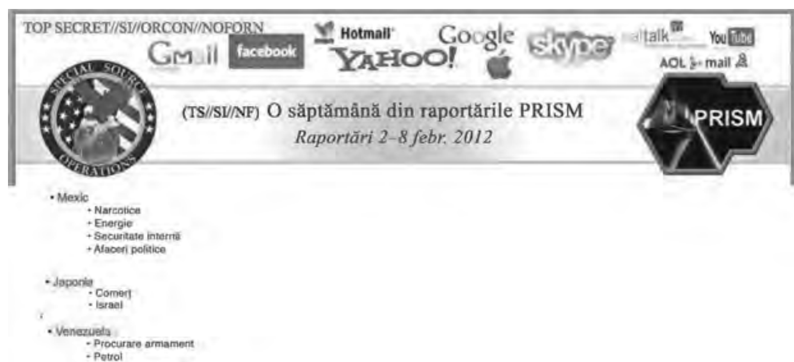
Clienți externi (Cine)	Cerințe privind informațiile (Ce)	Acces și tehnici de colectare (Cum)
Department of State	Counter Proliferation	DNI Strong Selectors
Central Intelligence Agency	Counter Terrorism	DNR Strong Selectors
United States UN Mission	Diplomatic	DNI Circuits
White House	Economic	DNR Circuits
Defense Intelligence Agency	Military	Mobile Wireless
National Counterterrorism Center	Political/Intention of Nations	

US-984 BLARNEY

(TS//SI) US-984 (PDDG: AX) – furnizează colectări de date împotriva comunicațiilor DNR și DNI autorizate prin deciziile Tribunalului FISA

(TS//SI) Ținte-cheie: instituții guvernamentale, contraterorism, guverne străine, entități economice

Dovezi ulterioare ale interesului economic al NSA apar într-un document PRISM care arată o „mostră“ de „Subiecte de raportat“ pentru săptămâna 2–8 februarie 2013. O listă cu tipurile de informaţii strânse din diverse ţări include în mod clar categorii economice și financiare, dintre care „energie“, „comerţ“ și „petrol“:



Un memorandum din 2006 din partea administratorului de capacităţi globale al misiunii agenţiei Probleme de Securitate Internaţională (ISI) descrie spionajul economic și comercial al NSA – împotriva unor ţări diverse ca Belgia, Japonia, Brazilia și Germania – în termeni clari:

(U) **Misiunea NSA Washington**

(U) **Regional**

(TS//SI) ISI este responsabilă de 13 state de pe trei continente. O caracteristică semnificativă care leagă aceste ţări este importanţa lor pentru preocupările economice, comerciale şi de apărare ale SUA. Divizia Europa Occidentală şi Parteneriatul Strategic se concentrează în primul rând pe politica externă şi activităţile comerciale ale Belgiei, Franţei, Germaniei, Italiei şi Spaniei, precum şi ale Braziliei, Japoniei şi Mexicului.

(TS//SI) Ramura Energie şi Resurse oferă informaţii unice despre producţia mondială de energie şi dezvoltarea unor ţări cheie care afectează economia mondială. Ţinte ale atenţiei actuale sunt [redacted] şi [redacted]. Raportarea a inclus monitorizarea investiţiilor internaţionale în sectoarele energiei din ţările vizate, a modernizărilor electrice şi a serviciului Monitorizare, Control şi Achiziţii de Date (SCADA) şi machetelor computerizate ale proiectelor energetice planificate.

Scriind despre un grup de documente ale GCHQ furnizate de Snowden, *New York Times*[27] a notat că ţintele supravegherii acestei agenţii includeau deseori instituţii financiare și „liderii unor organizaţii internaţionale de ajutor, companii energetice străine și oficiali ai Uniunii Europene implicaţi în lupte

antitrust cu firme tehnologice americane“. Acesta a adăugat că agenţiile americană și britanică „au monitorizat comunicaţiile unor oficiali UE de rang înalt, ale unor lideri străini, inclusiv șefi de stat africani, și uneori ale membrilor familiilor lor, ale unor directori ai Naţiunilor Unite și ale altor programe de asistenţă (precum UNICEF) și oficiali care supervizează ministerele petrolului și finanţelor“.

Motivul spionajului economic este suficient de clar. Când Statele Unite folosesc NSA pentru a urmări strategiile altor ţări în timpul negocierilor economice și comerciale, pot câștiga un avantaj enorm pentru industria americană. În 2009, de exemplu, asistentul secretarului de stat Thomas Shannon i-a trimis o scrisoare lui Keith Alexander, în care îi mulţumea și îi transmitea „felicitări pentru sprijinul remarcabil“ pe care Departamentul de Stat l-a primit în legătură cu cel de-al Cincilea Summit al Americilor, o conferinţă dedicată negocierii unor acorduri economice. În scrisoare, Shannon notează explicit că supravegherea NSA a oferit Statelor Unite avantaje în negociere în faţa altor participanţi:

> Cele peste 100 de raportări pe care le-am primit de la NSA ne-au oferit o perspectivă din interior asupra planurilor şi intențiilor altor participanți la summit şi au asigurat o bună pregătire a diplomaților noştri pentru ca aceştia să îi consilieze pe preşedintele Obama şi pe secretarul de stat Clinton în legătură cu modul în care să trateze probleme controversate, precum Cuba, şi să interacționeze cu interlocutori dificili, precum preşedintele venezuelean Chavez.

NSA este la fel de devotată și spionajului diplomatic, așa cum demonstrează un document referitor la „afacerile politice“. Un exemplu edificator, din 2011, arată cum agenţia a urmărit doi lideri latino-americani – Dilma Rousseff, președintele Braziliei, alături de „consilierii săi principali“; și Enrique Peña Nieto, candidatul principal la alegerile prezidenţiale din Mexic

de la momentul respectiv (în prezent președinte), alături de „nouă dintre asociaţii săi apropiaţi“ – într-o „intensificare“ a supravegherii deosebit de invazivă. Documentul prezintă chiar unele dintre mesajele text interceptate trimise și primite de Nieto și un „asociat apropiat“ al acestuia:

TOP SECRET//COMINT//REL TO USA, GBR, AUS, CAN, NZL

(U//FOUO) S2C42 efort intensificat

(U) Ţintă

(TS//SI//REL) O înţelegere sporită a metodelor de comunicare şi a selectorilor asociaţi preşedintelui brazilian Dilma Rousseff şi consilierilor săi principali.

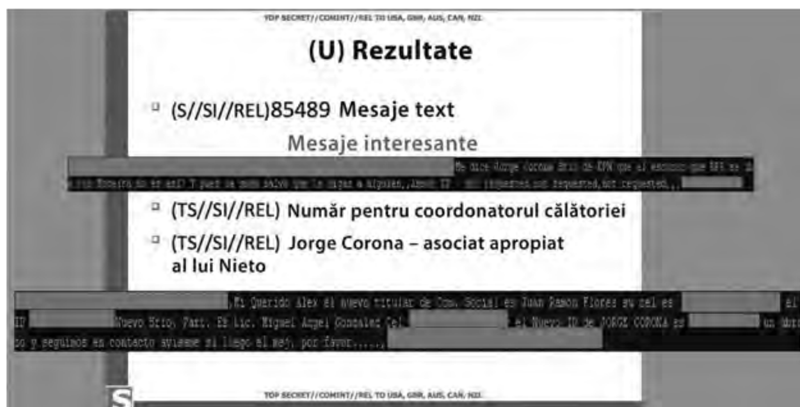
TOP SECRET//COMINT//REL TO USA, GBR, AUS, CAN, NZL

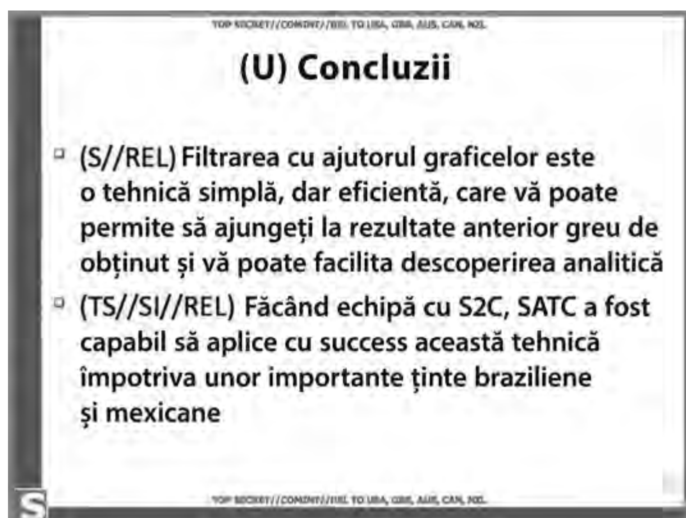
TOP SECRET//COMINT//REL TO USA, GBR, AUS, CAN, NZL

(U//FOUO) S2C41 efort intensificat

(TS//SI//REL) Echipa NSA din Mexic (S2C41) a desfăşurat un efort intensificat de urmărire de două săptămâni în privinţa unuia dintre candidaţii principali la alegerile prezidenţiale din Mexic, Enrique Peña Nieto, şi a nouă dintre asociaţii săi apropiaţi. Nieto este considerat de experţii politici cel mai probabil câştigător al alegerilor prezidenţiale din Mexic din 2012, care vor avea loc în iulie 2012. SATC a oferit analize grafice în eforturile de urmărire intensificată a ţintei.

TOP SECRET//COMINT//REL TO USA, GBR, AUS, CAN, NZL





Se poate specula cu privire la motivul pentru care liderii politici ai Braziliei și Mexicului au fost ţintele NSA. Ambele ţări sunt bogate în resurse de petrol, fiind o prezenţă influentă în regiune. Și, deși sunt departe de a fi adversari, ele nu sunt nici cei mai apropiaţi și mai de încredere aliaţi ai Americii. Într-adevăr, un document de planificare al NSA – intitulat „Identificarea Provocărilor: Tendinţe Geopolitice pentru

2014–2019“ – enumeră atât Brazilia, cât și Mexicul la capitolul „Prieteni, Inamici sau Probleme?“. Alte ţări prezente pe această listă sunt Egiptul, India, Iranul, Arabia Saudită, Somalia, Sudanul, Turcia și Yemenul.

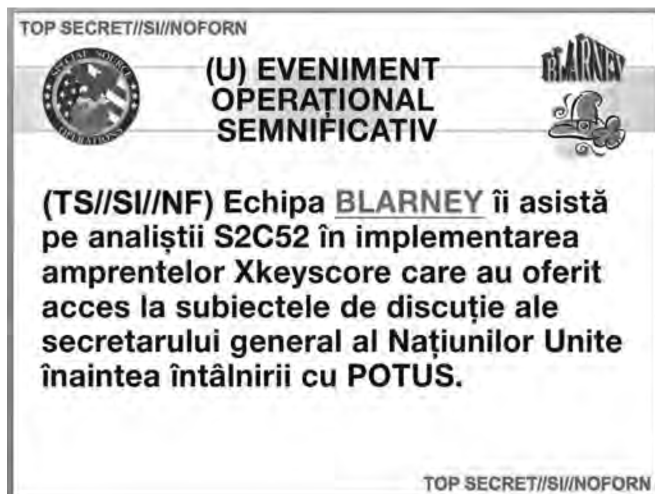
Dar în cele din urmă, în acest caz, ca și în majoritatea celorlalte, speculaţiile privind o ţintă specifică se bazează pe o premisă falsă. NSA nu are nevoie de nici un motiv anume pentru a viola comunicaţiile private ale oamenilor. Misiunea sa instituţională este să colecteze tot.

Însă dezvăluirile despre spionarea de către NSA a liderilor străini sunt *mai puţin* semnificative decât supravegherea în masă și fără mandat a întregii populaţii desfășurată de agenţie. Ţările i-au spionat pe șefii de stat secole la rând, inclusiv pe cei ai aliaţilor. Acest lucru nu este surprinzător, în pofida protestelor generate, de exemplu, de descoperirea că NSA a supravegheat timp de mulţi ani telefonul personal al cancelarului german Angela Merkel.

Mai remarcabil este faptul că, în ţările vizate, dezvăluirile că NSA a spionat sute de mii de cetăţeni ai acestora au produs doar niște mici obiecţii din partea conducerii politice a ţărilor respective. Indignarea reală a izbucnit după ce liderii respectivi au înţeles că și ei, nu numai cetăţenii lor, au fost vizaţi de această supraveghere.

Cu toate acestea, scara mare a supravegherii diplomatice practicate de NSA este neobișnuită și demnă de atenţie. În afară de liderii străini, Statele Unite au spionat, de exemplu, la scară mare organizaţii internaţionale precum Naţiunile Unite pentru a obţine avantaje diplomatice. O informare din aprilie 2013 din partea SSO este tipică, notând modul în care agenţia și-a folosit programele pentru a obţine subiectele generale de discuţie ale secretarului ONU înainte de întâlnirea acestuia cu președintele Obama.

Numeroase alte documente detaliază modul în care Susan Rice, pe atunci ambasador la ONU, iar în prezent consilier al președintelui Obama pentru securitate naţională, a cerut în



mod repetat ca NSA să spioneze discuţiile interne ale statelor membre cheie pentru a le afla strategiile de negociere. Un raport din mai 2010 al SSO descrie acest proces în legătură cu o rezoluţie aflată în dezbatere la ONU ce implica impunerea unor noi sancţiuni Iranului.

(S//SI) Echipa BLARNEY oferă sprijin substanţial pentru a permite colectarea la Consiliul de Securitate al ONU

De NUME REDACTAT la 2010-05-28 1430

(TS//SI//NF) În timp ce votul ONU pe tema sancţiunilor împotriva Iranului se apropie şi câteva ţări se opun luării unei decizii, ambasadorul Rice a apelat la NSA cerând SIGINT despre acele ţări, astfel încât să poată elabora o strategie. Cu solicitarea ca acest lucru să se facă rapid şi în cadrul autorităţii noastre legale, echipa BLARNEY a trecut la treabă cu organizaţiile şi partenerii NSA atât interni, cât şi externi.

(TS//SI//NF) În timp ce OGC, SV şi TOPI au lucrat agresiv la pregătirea documentelor legale pentru a urgenta patru noi ordine ale tribunalului FISA pentru Gabon, Uganda, Nigeria şi Bosnia, personalul din cadrul Diviziei pentru Operaţiuni a BLARNEY se află în spatele scenei colectând date care să stabilească anume ce informaţii sunt disponibile pentru supraveghere sau dacă acestea pot fi obţinute prin contactele consacrate ale FBI. În timp ce a lucrat pentru a obţine informaţii atât la Misiunea ONU din New York, cât şi la ambasadele din DC, echipa de urmărire a contribuit cu personal adecvat pentru transmiterea de date şi s-au făcut toate pregătirile pentru a asigura transmiterea datelor către TOPI cât mai repede posibil. Câteva persoane, una din echipa juridică şi una din echipa de urmărire, au fost chemate sâmbătă 22 mai pentru a participa la punerea la punct a documentelor legale în 24 de ore pentru ca ordinele să fie gata pentru a fi semnate de

```
în 24 de ore pentru ca ordinele să fie gata pentru a fi semnate de
directorul NSA în dimineaţa zilei de luni 24 mai.

(S//SI) În timp ce OGC şi SV fac presiuni pentru urgentarea acestor patru
ordine, ele au mers de la directorul NSA care le-a semnat la DoD* pentru
semnarea de către SECDEF** şi apoi la DOJ*** pentru semnarea de către judecăto-
rul FISC într-un timp record. Toate cele patru ordine au fost semnate de
judecător miercuri 26 mai! Imediat ce ordinele au fost primite de echipa
juridică a BLARNEY, aceasta a trecut la acţiune, analizând cele patru ordine
plus altă reînnoire „normală“ într-o zi. Analizarea celor cinci ordine
într-o zi - un record BLARNEY! În timp ce echipa juridică a BLARNEY analiza
ordinele judecătoreşti, echipa de management al accesului a BLARNEY lucra
cu FBI pentru a transmite informaţiile de căutat şi pentru a coordona colabo-
rarea cu partenerii din telecomunicaţii.
```

Un document de supraveghere similar din august 2010 dezvăluie că Statele Unite au spionat opt membri ai Consiliului de Securitate al ONU privind o rezoluţie ulterioară despre sancţiunile împotriva Iranului. Lista includea Franţa, Brazilia, Japonia și Mexic – toate considerate naţiuni prietene. Spionajul a furnizat administraţiei americane informaţii valoroase despre intenţiile de vot ale acestor ţări, oferind Washingtonului un avantaj atunci când a discutat cu alţi membri ai Consiliului de Securitate.

TOP SECRET//COMINT//NOFORN

August 2010



(U//FOUO) Succes discret: Sinergia SIGINT ajută la modelarea politicii externe a SUA

(TS//SI//NF) De la începutul acestor negocieri îndelungate, NSA a efectuat colectări de informaţii împotriva Franţei, Japoniei, Mexicului, Braziliei

(TS/SI/REL) La sfârşitul primăverii lui 2010 11 ramuri din cinci Linii de Producţie au lucrat cu facilitatorii NSA pentru a oferi cele mai actuale şi mai corecte informaţii USUN şi altor clienţi despre modul în care membrii UNSC vor vota în privinţa Rezoluţiei referitoare la sancţiunile împotriva Iranului. Menţionând că Iranul a continuat să nu se conformeze precedentelor rezoluţii ale UNSC privind programul său nuclear, ONU a impus sancţiuni suplimentare la 9 iunie 2010. SIGINT a fost un factor cheie în informarea USUN despre modul în care vor vota alţi membri ai UNSC.

(TS//SI//REL) Rezoluţia a fost adoptată cu 12 voturi pentru, două împotrivă (Brazilia şi Turcia) şi o abţinere din partea Libanului. Potrivit USUN, SIGINT „m-a ajutat să ştiu când alţi Permreps [reprezentanţi permanenţi] spuneau adevărul... şi-au dezvăluit poziţia reală în privinţa sancţiunilor... ne-au oferit un avantaj în negocieri... şi au oferit informaţii despre «limitele acceptabile» de diversele ţări"

* Departamentul Apărării (n.tr.)
** Secretarul Apărării (n.tr.)
*** Departamentul de Justiție (n.tr.)

Pentru a facilita spionajul diplomatic, NSA a câștigat diverse forme de acces la ambasadele și consulatele multora dintre aliații săi apropiați. Un document din 2010 – prezentat aici cu unele țări șterse – enumeră națiunile ale căror structuri diplomatice din interiorul Statelor Unite au fost violate de agenție. Un glosar de la sfârșit explică diversele tipuri de supraveghere folosite.

10 sep 2010

CLOSE ACCESS SIGADS

CLOSE ACCESS SIGADS

Toate colectările naționale utilizează US-3136 SIGAD, cu un sufix unic din două litere pentru fiecare locație și misiune ale țintei. Colectărilor internaționale GENIE le-a fost atribuit US-3137 SIGAD, cu un sufix din două litere.

(Notă: La țintele marcate cu * fie s-a renunțat, fie urmează să se renunțe în viitorul apropiat. Vă rugăm să verificați cu TAO/RTD/ROS (961-1578) cu privire la statutul autorităților.)

SIGAD US-3136

SUFFIX	TARGET/COUNTRY	LOCATION	COVERTERM	MISSION
BE	Brazil/Emb	Wash,DC	KATEEL	LIFESAVER
SI	Brazil/Emb	Wash,DC	KATEEL	HIGHLANDS
VQ	Brazil/UN	New York	POCOMOKE	HIGHLANDS
HN	Brazil/UN	New York	POCOMOKE	VAGRANT
LJ	Brazil/UN	New York	POCOMOKE	LIFESAVER
YL *	Bulgaria/Emb	Wash, DC	MERCED	HIGHLANDS
QX *	Colombia/Trade Bureau	New York	BANISTER	LIFESAVER
DJ	EU/UN	New York	PERDIDO	HIGHLANDS
SS	EU/UN	New York	PERDIDO	LIFESAVER
KD	EU/Emb	Wash, DC	MAGOTHY	HIGHLANDS
IO	EU/Emb	Wash, DC	MAGOTHY	MINERALIZ
XJ	EU/Emb	Wash,DC	MAGOTHY	DROPMIRE
OF	France/UN	New York	BLACKFOOT	HIGHLANDS
VC	France/UN	New York	BLACKFOOT	VAGRANT
UC	France/Emb	Wash, DC	WABASH	HIGHLANDS

UC	France/Emb	Wash, DC	WABASH	HIGHLANDS
LO	France/Emb	Wash, DC	WABASH	PBX
NK *	Georgia/Emb	Wash, DC	NAVARRO	HIGHLANDS
BY *	Georgia/Emb	Wash, DC	NAVARRO	VAGRANT
RX	Greece/UN	New York	POWELL	HIGHLANDS
HB	Greece/UN	New York	POWELL	LIFESAVER
CD	Greece/Emb	Wash, DC	KLONDIKE	HIGHLANDS
PJ	Greece/Emb	Wash,DC	KLONDIKE	LIFESAVER
JN	Greece/Emb	Wash, DC	KLONDIKE	PBX
MO*	India/UN	New York	NASHUA	HIGHLANDS
QL *	India/UN	New York	NASHUA	MAGNETIC
ON *	India/UN	New York	NASHUA	VAGRANT
IS *	India/UN	New York	NASHUA	LIFESAVER
OX *	India/Emb	Wash,DC	OSAGE	LIFESAVER
CQ *	India/Emb	Wash, DC	OSAGE	HIGHLANDS
TQ *	India/Emb	Wash, DC	OSAGE	VAGRANT
CU *	India/EmbAnx	Wash, DC	OSWAYO	VAGRANT
DS *	India/EmbAnx	Wash, DC	OSWAYO	HIGHLANDS
SU *	Italy/Emb	Wash, DC	BRUNEAU	LIFESAVER
MV *	Italy/Emb	Wash, DC	HEMLOCK	HIGHLANDS
IP *	Japan/UN	New York	MULBERRY	MINERALIZ
HF *	Japan/UN	New York	MULBERRY	HIGHLANDS
BT *	Japan/UN	New York	MULBERRY	MAGNETIC
RU *	Japan/UN	New York	MULBERRY	VAGRANT
LM *	Mexico/UN	New York	ALAMITO	LIFESAVER
UX *	Slovakia/Emb	Wash, DC	FLEMING	HIGHLANDS
SA *	Slovakia/Emb	Wash, DC	FLEMING	VAGRANT
XR *	South Africa/ UN & Consulate	New York	DOBIE	HIGHLANDS
RJ *	South Africa/ UN & Consulate	New York	DOBIE	VAGRANT
YR *	South Korea/UN	New York	SULPHUR	VAGRANT
TZ *	Taiwan/TECO	New York	REQUETTE	VAGRANT
VN *	Venezuela/Emb	Wash, DC	YUKON	LIFESAVER
UR *	Venezuela/UN	New York	WESTPORT	LIFESAVER
NO *	Vietnam/UN	New York	NAVAJO	HIGHLANDS
OU *	Vietnam/UN	New York	NAVAJO	VAGRANT
GV *	Vietnam/Emb	Wash, DC	PANTHER	HIGHLANDS

SIGAD US-3137

DESCRIERE TERMENI GENERALI

HIGHLANDS: Colectare din implanturi
VAGRANT: Colectare de capturi de ecran
MAGNETIC: Colectare a emisiilor magnetice prin intermediul senzorilor
MINERALIZE: Colectare de la implanturi LAN
OCEAN: Sistem de colectare optică pentru capturi de ecran alcătuite din raster
LIFESAVER: Copii ale hard-disk-ului
GENIE: Funcționare etapizată; accesarea rețelelor securizate prin izolare
BLACKHEART: Colectare din implanturi FBI
PBX: Switch-uri de sisteme telefonice
CRYPTO ENABLED: Colectare derivată din eforturile de activare a criptării prin Opţiunea de Autentificare (AO)
DROPMIRE: Colectare pasivă a emisiilor unei antenă
CUSTOMS: Oportunități uzuale (fără legătură cu LIFESAVER)
DROPMIRE: Colectare de la imprimantele laser, doar prin acces din proximitate (FĂRĂ implanturi)
DEWSWEEPER: Hardware USB gazdă ce furnizează o conexiune COVERT prin intermediul unei conexiuni USB către o rețea țintă. Funcționează printr-un subsistem de relee W/RF pentru a furniza o conexiune de tip bridge wireless către rețeaua țintă.
RADON: Dispozitiv gazdă bidirecțional care poate injecta pachete Ethernet în aceeași țintă. Permite exploatarea bidirecțională a rețelelor marcate cu Acces Interzis folosind aplicații standard de rețea.

Unele dintre metodele NSA servesc tuturor agendelor – economică, diplomatică, de securitate și obţin un avantaj global utilizabil în orice condiţii –, iar acestea sunt printre cele mai invazive și ipocrite din repertoriul agenţiei. Ani la rând, administraţia SUA a avertizat zgomotos lumea că routerele chinezești și alte dispozitive de internet reprezintă o „ameninţare“ pentru că sunt construite cu o funcţie de supraveghere ascunsă ce oferă guvernului chinez capacitatea de a spiona pe oricine le folosește. Ceea ce arată documentele NSA este că americanii au fost implicaţi tocmai în activitatea de care Statele Unite au acuzat China că o desfășoară.

Acuzaţiile americane împotriva dispozitivelor de internet fabricate în China au fost dure. În 2012, de exemplu, un raport al Comisiei pentru Serviciile de Informaţii din Camera

Reprezentanţilor, prezidată de Mike Rogers, pretindea că Huawei și ZTE,[28] cele mai importante două companii chineze de telecomunicaţii, „este posibil să încalce legile Statelor Unite“ și că „nu au respectat obligaţiile legale americane sau standardele internaţionale privind conduita în afaceri“. Comisia a recomandat ca „Statele Unite să privească cu suspiciune penetrarea continuă a pieţei americane de telecomunicaţii de către companiile de telecomunicaţii chineze“.

Comisia Rogers a exprimat temeri potrivit cărora cele două companii permit supravegherea de stat a Chinei, deși a recunoscut că nu a obţinut nici o dovadă că firmele au implantat routerele sau alte sisteme ale lor cu dispozitive de supraveghere. Cu toate acestea, a citat eșecul acestor companii de a coopera și a cerut firmelor americane să evite cumpărarea produselor lor:

> Entitățile din sectorul privat din Statele Unite sunt puternic încurajate să ia în considerare riscurile de securitate pe termen lung asociate cu afacerile cu ZTE sau Huawei pentru echipament sau servicii. Furnizorii de rețea americani şi dezvoltatorii de sisteme sunt puternic încurajați să caute alți vânzători pentru proiectele lor. Pe baza informațiilor disponibile secretizate şi nesecretizate, Huawei şi ZTE nu pot fi de încredere în ceea ce priveşte influența externă şi reprezintă o amenințare de securitate pentru Statele Unite şi sistemele noastre.

Acuzaţiile constante au devenit o povară atât de mare, încât Ren Zhengfei, fondatorul și directorul general al Huawei, în vârstă de 69 de ani, a anunţat în noiembrie 2013 că abandonează piaţa americană. Așa cum relata *Foreign Policy*[29], Zhengfei a afirmat pentru un ziar franţuzesc: „Dacă Huawei ajunge în mijlocul relaţiilor SUA–China și provoacă probleme, nu merită“.

Dar în timp ce companiile americane au fost avertizate în privinţa routerelor chinezești presupuse a nu fi de încredere, organizaţiile străine ar fi trebuit avertizate să fie atente la cele de fabricaţie americană. Un raport din iunie 2010 al șefului

Departamentului NSA de Dezvoltare de Acces și Ținte este șocant de explicit. NSA primește în mod curent – sau interceptează – routere, servere și alte dispozitive ale reţelelor de calculatoare exportate din Statele Unite înainte de a fi trimise clienţilor internaţionali. Agenţia implantează instrumente de supraveghere ascunse, resigilează dispozitivele și le trimite. NSA obţine astfel acces la toate reţelele și utilizatorii lor. Documentul observă bucuros că unele „tradecraft SIGINT... sunt foarte practice“:

TOP SECRET//COMINT//NOFORN

Iunie 2010



(U) Tehnicile ascunse pot să ajungă la unele dintre cele mai dificile ţinte ale SIGINT

De: (U//FOUO) NUME REDACTAT Şef, Dezvoltare Acces și Ţintă (S3261)



(TS//SI//NF) Nu toate tradecraft SIGINT presupun accesarea semnalelor și reţelelor de la mii de kilometri depărtare... De fapt, uneori este foarte practic. Iată cum funcționează: transporturile de dispozitive pentru reţelele de calculatoare (servere, routere etc.) livrate ţintelor noastre din întreaga lume sunt interceptate. Apoi sunt redirecţionate către un loc secret unde angajaţii Diviziei Operaţiuni de Acces la Comandă/Operaţiuni de Acces (AO – S326), cu sprijinul Centrului de Operaţiuni la Distanţă (S321), permit instalarea unor implanturi de semnal direct în dispozitivele electronice ale ţintelor noastre. Aceste dispozitive sunt apoi reasamblate și plasate din nou în tranzit către destinaţia iniţială. Toate acestea se întâmplă cu spriijinul partenerilor Comunităţii de Informaţii și asistenţilor tehnici din TAO.

(TS//SI//NF) Astfel de operaţiuni ce implică interceptarea lanţului de aprovizionare sunt unele dintre cele mai productive operaţiuni din TAO, pentru că prepoziţionează puncte de acces la reţele greu de urmărit din lume.





(TS//SI//NF) Stânga: Pachetele interceptate sunt deschise cu atenţie;
Dreapta: O „staţie de încărcare“ implantează un semnal.

În cele din urmă, dispozitivul modificat se conectează din nou la infrastructura NSA:

(TS//SI//NF) Într-un caz recent, după câteva luni, un semnal implantat a emis din nou către infrastructura acoperită a NSA. Această emitere ne-a oferit acces suplimentar la exploatarea dispozitivului și supravegherea rețelei.

Printre alte dispozitive, agenţia interceptează și modifică routere și servere fabricate de Cisco pentru a direcţiona o cantitate mare a traficului pe internet către stocurile de date ale NSA. (Nu există dovezi în documente că Cisco știe sau că a coordonat aceste interceptări.) În aprilie 2013, agenţia a întâmpinat dificultăţi tehnice privind switchurile (comutatorii) de reţea Cisco interceptate, care au afectat programele BLARNEY, FAIRVIEW, OAKSTAR și STORMBREW:

TOP SECRET//COMINT//REL TO USA, FVEY
(Report generated on:4/11/2013 3:31:06PM)

NewCrossProgram — Active ECP Count: 1

CrossProgram-1-13 — New — ECP Lead:

Titlul schimbării: Update Software on all Cisco ONS Nodes

Expeditor: — Approval Priority: C-Routine

Site(-uri): APPLE1 : CLEVERDEVICE : HOMEMAKER : DOGHUT : QUARTERPOUNDER : QUEENSLAND : SCALLION : SPORTCOAT : SUBSTRATUM : TITAN POINTE : SUBSTRATUM : BIRCHWOOD : MAYTAG : EAGLE : EDEN : — Project(s): No Project(s) Entered

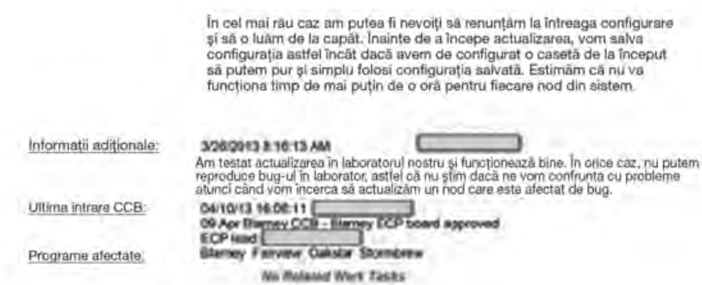
Sisteme: Comms/Network : Comms/Network : Comms/Network : Comms/Network : — Subsystem(s): No Subsystem(s) Entered

Descrierea schimbării: Actualizarea software-ului pentru toate switch-urile de reţea optică Cisco

Motivul schimbării: Toate multiplexoarele noastre Cisco ONS SONET se confruntă cu un bug în software care le face să se întrerupă intermitent

Impactul misiunii: Impactul misiunii nu este cunoscut. În timp ce bug-ul nu pare să afecteze traficul, reactualizarea software-ului poate face acest lucru. Nu putem simula bug-ul în laboratorul nostru, astfel că este imposibil de anticipat cu exactitate ce se va întâmpla în momentul în care vor face reactualizarea. Propunem actualizarea unuia dintre noduri în NBP-320 mai întâi pentru a stabili dacă actualizarea se desfășoară fără probleme.

Recent am încercat să resetăm cardul de gestionare a modului standby în nodul HOMEMAKER. Când acest lucru a eșuat, am încercat să îl resetăm fizic. De vreme ce era cardul de standby, nu ne așteptam să apară probleme. Totuși, după resetarea cardului, întreaga ONS s-a prăbușit și am pierdut tot traficul prin casetă. A durat mai mult de o oră pentru revenirea la normal după acest eșec.



În cel mai rău caz am putea fi nevoiți să renunțăm la întreaga configurare și să o luăm de la capăt. Înainte de a începe actualizarea, vom salva configurația astfel încât dacă avem de configurat o casetă de la început să putem pur și simplu folosi configurația salvată. Estimăm că nu va funcționa timp de mai puțin de o oră pentru fiecare nod din sistem.

Informații adiționale: 3/26/2013 8:16:13 AM [redacted]
Am testat actualizarea în laboratorul nostru și funcționează bine. În orice caz, nu putem reproduce bug-ul în laborator, astfel că nu știm dacă ne vom confrunta cu probleme atunci când vom încerca să actualizăm un nod care este afectat de bug.

Ultima intrare CCB: 04/10/13 16:06:11 [redacted]
09 Apr Blarney CCB - Blarney ECP board approved
ECP lead [redacted]

Programe afectate: Blarney Fairview Oakstar Stormbrew

No Related Work Tasks

Este posibil ca firmele chinezești să implanteze mecanisme de supraveghere în dispozitivele lor de rețea. Dar Statele Unite fac cu siguranță acest lucru.

Să avertizezi lumea în legătură cu supravegherea chineză ar putea fi unul dintre motivele din spatele afirmațiilor administrației americane că dispozitivele chinezești nu sunt de încredere. Dar un motiv la fel de important pare să fie împiedicarea dispozitivelor chinezești să le înlocuiască pe cele de fabricație americană, ceea ce ar limita accesul NSA. Cu alte cuvinte, routerele și serverele chinezești reprezintă nu numai o competiție economică, ci și o competiție în supraveghere: când cineva cumpără un dispozitiv chinezesc în locul unuia american, NSA pierde un mijloc crucial de spionare a unui număr mare de activități de comunicare.

Cantitatea colectărilor dezvăluită era deja uimitoare, însă misiunea NSA de a colecta toate semnalele în permanență a determinat agenția să se extindă și să câștige mai mult teren. Cantitatea de date pe care o colectează este atât de mare, în realitate, încât principala provocare de care se plânge agenția este stocarea grămezilor de informații acumulate din întreaga lume. Un document al NSA pregătit pentru Conferința SigDev a alianței Five Eyes prezintă această problemă fundamentală:

TOP SECRET//COMINT//REL TO USA, FVEY

Provocarea

Colectarea depășește capacitatea noastră de acumulare, procesare și stocare conform „normelor" cu care ne-am obișnuit.

Povestea datează din 2006, când agenția a început ceea ce a numit „Extinderea la scară largă a partajării de metadate ale NSA". La acel moment, NSA anticipa că volumul de metadate colectate va crește cu șase sute de miliarde de date în fiecare an, creștere care ar include unul până la două miliarde de noi cazuri de apeluri telefonice colectate într-o singură zi:

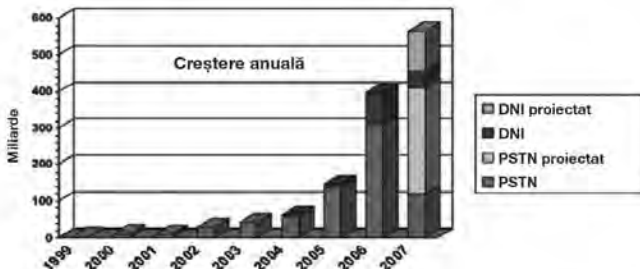
SECRET//COMINT//REL TO USA, FVEY//20320108



Extindere la scară lagă a partajării de metadate ale NSA



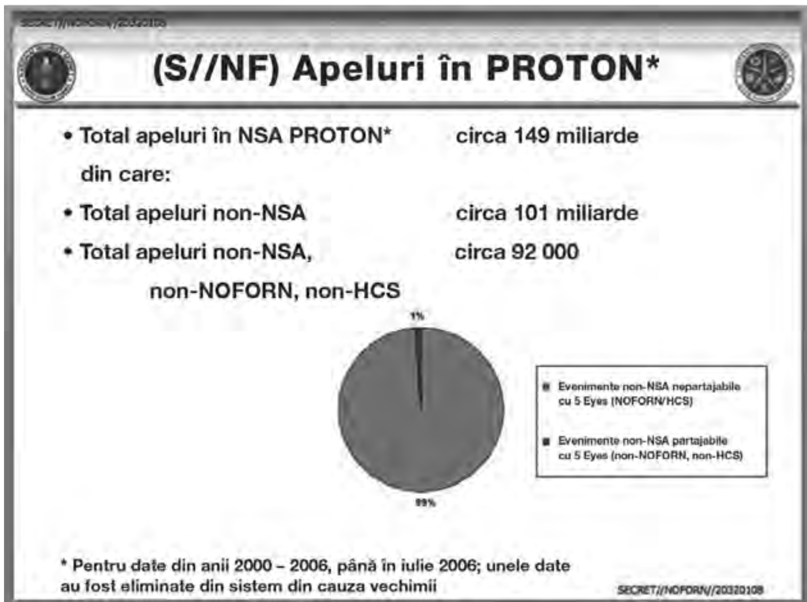
(S//SI//REL) Creșterea partajării de metadate din comunicații ale NSA de la 50 de miliarde de înregistrări la peste 850 de miliarde de înregistrări (creșteri de 1–2 miliarde de înregistrări pe zi)



**(C//REL) Include apeluri de la parteneri SIGINT de rang secund (circa 126 miliarde de înregistrări)*

SECRET//COMINT//REL TO USA, FVEY//20320108

Până în mai 2007, extinderea și-a arătat în mod evident roadele: cantitatea de metadate telefonice pe care le stoca agenția – independent de e-mailuri și de alte date de internet și excluzând datele pe care NSA le ștersese din lipsă de spațiu de stocare – crescuse la 150 de miliarde de date:



Odată ce au fost adăugate și comunicațiile prin internet, numărul total al cazurilor de comunicare stocat s-a apropiat de un trilion (ar trebui subliniat că aceste date erau partajate de NSA cu alte agenții).

Pentru a face față acestei probleme de stocare, NSA a început să construiască o nouă instalație masivă în Bluffdale, Utah, care are ca principal scop stocarea tuturor datelor. Așa cum menționa reporterul James Bamford[30] în 2012, construcția din Bluffdale va extinde capacitatea agenției prin adăugarea a „patru săli de 2 322 de metri pătrați pline cu servere, cărora

li se adaugă un spaţiu la etaj pentru cabluri și depozitare. În plus, vor fi peste 83 600 metri pătraţi pentru suport tehnic și administrare". Având în vedere mărimea clădirii și faptul că, așa cum spune Bamford, „un terabyte de date poate fi stocat acum pe o unitate de mărimea degetului mic", implicaţiile colectării de date sunt profunde.

Necesitatea unor instalaţii și mai mari este deosebit de presantă având în vedere intruziunile curente ale agenţiei în activitatea globală online, care se extinde dincolo de colectarea de metadate pentru a include conţinutul e-mailurilor, navigarea pe internet, istoricul căutărilor și discuţiile pe chat. Programul cheie folosit de NSA pentru a colecta, organiza și căuta astfel de date, introdus în 2007, este X-KEYSCORE și permite un salt radical pentru puterile de supraveghere ale agenţiei. NSA numește X-KEYSCORE sistemul „cu cea mai mare rază de acţiune" pentru colectarea datelor electronice, și pe bună dreptate.

Un document de instruire pregătit pentru analiști afirmă că programul înregistrează „aproape orice face un utilizator obișnuit pe internet", inclusiv textul e-mailurilor, căutările pe Google și numele website-urilor vizitate. X-KEYSCORE permite chiar monitorizarea „în timp real" a activităţilor online ale unei persoane, permiţând NSA să vadă e-mailurile și activităţile de navigare pe măsură ce au loc.

Dincolo de colectarea unor date cuprinzătoare despre activităţile online a sute de milioane de persoane, X-KEYSCORE permite oricărui analist al NSA să caute în bazele de date ale sistemului după adresă de e-mail, număr de telefon sau atribute de identificare precum adresa IP. Gama de informaţii disponibile și mijloacele elementare pe care le folosește un analist pentru a căuta sunt ilustrate în acest slide:



Un alt slide despre X-KEYSCORE prezintă diferite câmpuri de informaţie care pot fi căutate prin „plug-in-urile" programului. Acestea includ „fiecare adresă de e-mail văzută într-o sesiune", „fiecare număr de telefon văzut într-o sesiune" (inclusiv „intrările din agendă") și „activitatea pe webmail și chat":

TOP SECRET//COMINT//REL TO USA, AUS, CAN, GBR, NZL

Plug-in-uri

KEYSCORE

Plug-in	DESCRIERE
Adrese de e-mail	Indexează fiecare adresă de e-mail văzută într-o sesiune după numele utilizatorului și după domeniu
Fișiere extrase	Indexează fiecare fișier văzută într-o sesiune după numele fișierului și după extensie
Logare completă	Indexează fiecare sesiune DNI colectată. Datele sunt indexate după IP, Port etc.
Analizor HTTP	Indexează traficul HTTP din partea clientului (urmează exemple)
Număr de telefon	Indexează fiecare număr de telefon văzut într-o sesiune (ex. intrări într-o agendă cu adrese)
Activitatea utilizatorului	Indexează activitatea de webmail și chat pentru a include numele utilizatorului, lista de prieteni, cookie-uri etc.

TOP SECRET//COMINT//REL TO USA, AUS, CAN, GBR, NZL

Programul oferă, de asemenea, posibilitatea de căutare și recuperare a documentelor și imaginilor încorporate care au fost create, trimise sau primite:

TOP SECRET//COMINT//ORCON,REL TO USA, AUS, CAN, GBR and NZL//20291123

KEYSCORE

Exemple de plug-in-uri „avansate"

Plug-in	DESCRIERE
Activitatea utilizatorului	Indexează activitatea de webmail și chat pentru a include numele utilizatorului, lista de prieteni, cookie-uri etc. (Exploatarea este făcută de AppProc)
Metadate din document	Extrag proprietățile fișierelor Microsoft Office și pe cele ale pdf-urilor Adobe, cum ar fi autorul, organizația, data la care au fost create etc.

Alte slide-uri ale NSA declară în mod deschis ambiția X-KEYSCORE de a cuprinde tot la nivel global:

De ce suntem interesați de HTTP?

facebook
YAHOO!
twitter
myspace.com
a place for friends

Pentru că aproape toate activitățile unui utilizator tipic de internet folosesc HTTP

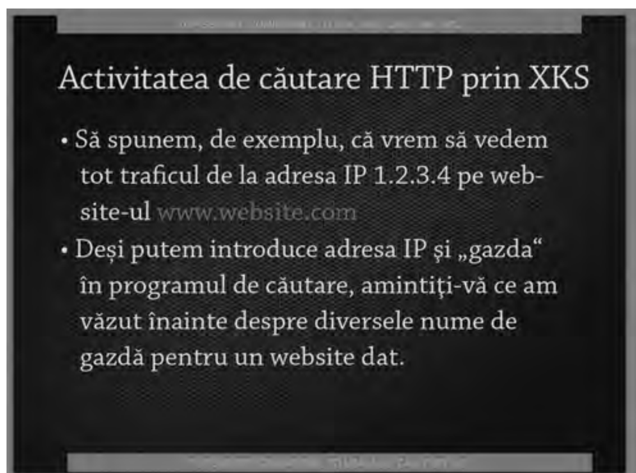
CNN.com
Google Earth
Gmail
@mail.ru
WIKIPEDIA
The Free Encyclopedia

- Aproape toate activităţile pe internet folosesc HTTP:
  - navigare pe internet
  - Webmail (Yahoo/Hotmail/Gmail/etc.)
  - OSN (Facebook/MySpace/etc.)
  - Căutare pe internet (Google/Bing/etc.)
  - Cartografiere online (Google Maps/Mapquest/etc.)

Căutările permise de program sunt atât de precise încât orice analist al NSA este capabil nu numai să găsească rapid ce website a vizitat o persoană, ci și să întocmească o listă cuprinzătoare cu toate vizitele pe un anumit website de pe anumite computere:

Activitatea de căutare HTTP prin XKS

O altă solicitare comună este reprezentată de faptul că analiştii vor să vadă tot traficul de pe o adresă IP dată (sau adrese IP) pe un website specific.



Este remarcabilă ușurința cu care analiștii pot căuta orice vor fără nici o supervizare. Un analist cu acces la X-KEYSCORE nu trebuie să depună o cerere către un supervizor sau o altă autoritate. Analistul completează doar un formular de bază pentru a „justifica“ supravegherea, iar sistemul îi oferă informațiile cerute.

TOP SECRET//COMINT//REL TO USA, AUS, CAN, GBR, NZL

Crearea căutărilor de adrese de e-mail

■ Introducerea utilizatorilor și a domeniilor în spațiile de căutare

Search: Email Addresses
Query Name: kmkeith_2
Justification: sqi in iran sample
Additional Justification:
Miranda Number:
Datetime: 1 Day Start: 2009-06-23 00:00 Stop:
Email Username: badguy or baddude1 or badguysemail
@Domain: yahoo.com
Subject:

Mulitiple usernames from SAME domain can be OR'd

TOP SECRET//COMINT//REL TO USA, AUS, CAN, GBR, NZL

În primul interviu video pe care l-a acordat când era în Hong Kong, Edward Snowden a făcut o afirmaţie îndrăzneaţă: „Stând la biroul meu, pot să interceptez pe oricine, de la tine sau contabilul tău până la un judecător federal sau chiar până la președinte, dacă am un e-mail personal". Oficialii americani au negat vehement că acest lucru ar fi adevărat. Mike Rogers l-a acuzat în mod expres pe Snowden că „minte", adăugând că „este imposibil să facă ceea ce spune că poate face". Dar X-KEYSCORE permite unui analist să facă exact ce a spus Snowden: să selecteze ca ţintă orice utilizator pentru o monitorizare cuprinzătoare, care include citirea conţinutului e-mailurilor acestuia. Într-adevăr, programul îi permite unui analist să caute toate e-mailurile care includ utilizatorii vizaţi în câmpul „cc" sau îi menţionează în corpul textului.

Instrucţiunile de căutare în e-mailuri ale NSA demonstrează cât de simplu și ușor este pentru analiști să monitorizeze orice persoană a cărei adresă o știu:

TOP SECRET//COMINT//REL TO USA, AUS, CAN, GBR, NZL//20320108

Căutare după adresa de e-mail:
Una dintre cele mai comune solicitări de căutare este (aţi ghicit) Email Adress Query, care caută după o adresă de e-mail. Pentru a crea o solicitare pentru o adresă de e-mail specifică, trebuie să completezi numele solicitării, să o justifici şi să selectezi o perioadă, apoi pur şi simplu să introduci adresa sau adresele de e-mail pe care vrei să le cauţi şi să trimiţi solicitarea.

Va arăta astfel…

Search: Email Addresses

Query Name: abujihad
Justification: ct target in n africa
Additional Justification:
Miranda Number:
Datetime: 1 Month Start: 2008-12-24 00:00
Email Username: abujihad
@Domain: yahoo.com

Una dintre cele mai valoroase funcţii ale X-KEYSCORE pentru NSA este capacitatea acestuia de a supraveghea activităţile pe reţelele de socializare (OSN), cum ar fi Facebook și Twitter, despre care agenţia crede că furnizează o bogăţie de informaţii și „o perspectivă de interior asupra vieţii personale a ţintei“:

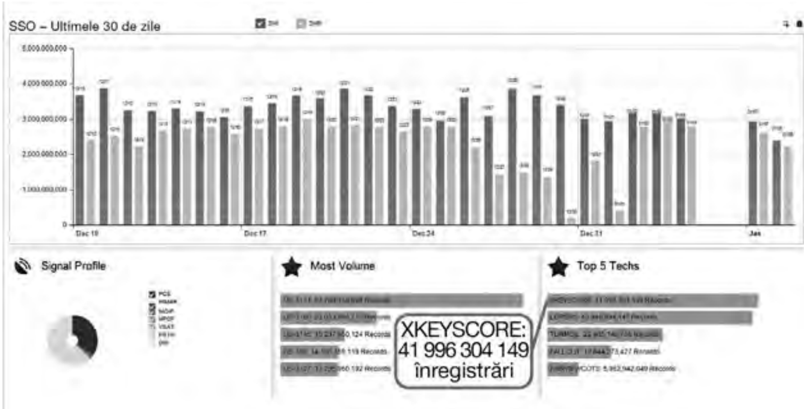


Metodele de căutare a activităţii de social media sunt la fel de simple ca și căutarea după e-mail. Un analist introduce numele de utilizator dorit pe Facebook, să zicem, împreună cu perioada activităţii, iar X-KEYSCORE returnează toate



informaţiile despre acel utilizator, inclusiv mesaje, discuţii online și alte postări private.

Poate faptul cel mai remarcabil în legătură cu X-KEYSCORE este cantitatea imensă de date pe care le capturează și le stochează în zone de colectare multiple din lume. „În unele zone“, afirmă un raport, „cantitatea de date pe care o primim pe zi (peste 20 de terabytes) poate fi stocată doar pentru 24 de ore pe baza resurselor disponibile“. Pe o perioadă de 30 de zile începând din decembrie 2012, cantitatea de date colectate de X-KEYSCORE pentru o divizie, SSO, depășește 41 de miliarde:



X-KEYSCORE „stochează conţinutul integral pentru 3–5 zile, încetinind efectiv internetul“ – ceea ce înseamnă că „analiștii pot reveni și recupera sesiunile“. Apoi „conţinutul de «interes» poate fi extras din X-KEYSCORE și trimis către Agility sau PINWALE“, baze de date ce oferă stocare pe termen lung.



Capacitatea X-KEYSCORE de a accesa Facebook și alte site-uri de socializare este amplificată de alte programe, inclusiv BLARNEY, permițând NSA să monitorizeze o „gamă extinsă de date Facebook prin activități de supraveghere și căutare“:

(TS//SI//NF) BLARNEY exploatează rețeaua de socializare prin colectarea extinsă Facebook

De NUME REDACTAT la 2011-03-14 0737

(TS//SI//NF) Evidențiere SSO – BLARNEY exploatează rețeaua de socializare prin colectarea extinsă Facebook

(TS//SI//NF) La 11 martie 2011, BLARNEY a început să furnizeze conținut Facebook îmbunătățit în mod substanțial și mult mai complet. Acesta este un mare salt înainte pentru capacitatea NSA de a exploata Facebook prin folosirea autorităților FISA și FAA. Acest efort a fost inițiat în parteneriat cu FBI în urmă cu șase luni pentru a redresa un sistem de colectare incompletă de pe Facebook. NSA poate acum să acceseze o gamă largă de date Facebook prin activități de supraveghere și căutare. OPI sunt încântați în legătură cu primirea multor domenii de conținut, cum ar fi chat-ul, pe o bază susținută, care anterior fusese disponibilă doar ocazional. O parte din conținut va fi complet nouă, inclusiv înregistrări video ale abonaților. În ansamblu, noua colectare de date Facebook va oferi o oportunitate SIGINT solidă împotriva țintelor noastre – de la geolocalizare bazată pe adresele lor IP și agent utilizator la colectarea tuturor mesajelor lor private și a informațiilor din profil. Multiple elemente din NSA au colaborat pentru asigurarea transmiterii cu succes a acestor date. Un reprezentant al NSA la FBI a coordonat dezvoltarea rapidă a sistemului de colectare; echipa PRINTAURA a SSO a scris un nou software și a făcut schimbări de configurare; CES a modificat protocolul său de exploatare a sistemelor, iar Direcția Tehnologie a accelerat actualizarea instrumentelor de prezentare a datelor astfel încât OPI să vadă datele în mod corespunzător.

Între timp, în Marea Britanie, Divizia de Exploatare Globală a Telecomunicaţiilor (GTE) din cadrul GCHQ a dedicat, de asemenea, resurse semnificative sarcinii, fapt detaliat într-o prezentare din 2011 de la conferinţa anuală a alianţei Five Eyes.

TOP SECRET//SI//REL FVEY

GCHQ

GTE

Exploatarea traficului pe Facebook în mediul inactiv pentru a obține informații specifice.

NAME REDACTED Capability Developer
Global Telecommunications Exploitation (GTE)
GCHQ

TOP SECRET//SI//REL FVEY

CONTACT INFORMATION REDACTED

TOP SECRET//SI//REL FVEY

GCHQ

GTE

De ce ONS?

- Folosirea tot mai frecventă de către ţinte a Facebook, BEBO, MySpace etc.
- O sursă de informare foarte bogată despre ţinte:
  - Detalii personale
  - „Tipar de viaţă"
  - Conexiuni cu asociaţi
  - Media

TOP SECRET//SI//REL FVEY
This information is exempt from disclosure under the Freedom of Information Act 2000 and may be subject to exemption under other UK information legislation. Refer disclosure requests to GCHQ on
CONTACT INFORMATION REDACTED

TOP SECRET//SI//REL FVEY

GCHQ

Căutare
în mediul inactiv

GTE

• Multe ţinte pe Facebook îşi blochează profilul, astfel că nu este posibil să vezi toate informaţiile…

Dar mediul inactiv oferă oportunitatea de a colecta aceste informaţii prin exploatarea slăbiciunilor inerente ale modelului de securitate al Facebook.

TOP SECRET//SI//REL FVEY

This information is exempt from disclosure under the Freedom of Information Act 2000 and may be subject to exemption under other UK information legislation. Refer disclosure requests to GCHQ on CONTACT INFORMATION REDACTED

În particular, GCHQ a găsit vulnerabilităţi în sistemul reţelei pentru stocarea fotografiilor, care poate fi folosit pentru obţinerea accesului la identităţile Facebook și albume de fotografii:



TOP SECRET//SI//REL FVEY

GCHQ

Exploatarea CDN FB

GTE

- Slăbiciuni
  - Autentificare fictivă
  - Securitate prin anonimat

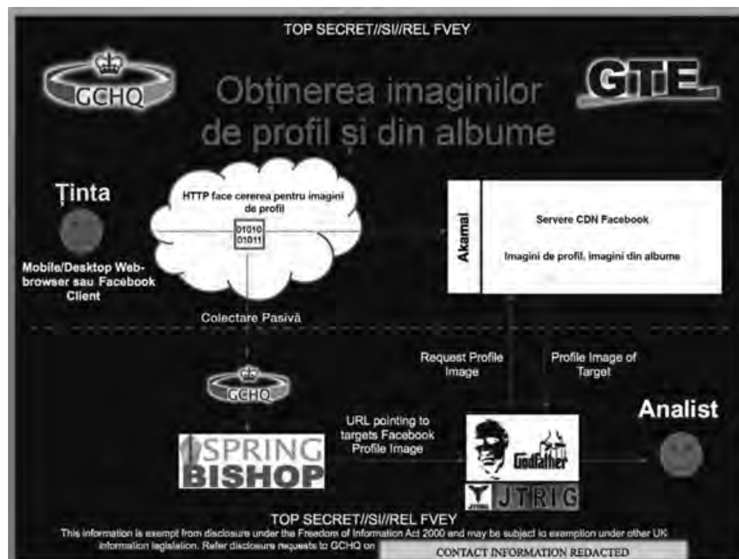
Este posibilă disecarea CDN din URL-ul generat de Facebook pentru a extrage ID-ul de utilizator Facebook al utilizatorului la a cărui imagine este atașat fișierul. De exemplu, mai jos este URL-ul pentru o imagine de profil tipică:

profile.ak.fbcdn.net EDITAT

Textul evidențiat cu gri-închis face referire la un anumit server din cadrul CDN Facebook, iar textul evidențiat cu gri-deschis este ID-ul de Facebook al utilizatorului

TOP SECRET//SI//REL FVEY

CONTACT INFORMATION REDACTED



Dincolo de rețelele de socilizare, NSA și GCHQ continuă să caute orice lacună în supravegherea lor, orice comunicare care rămâne în afara capacității lor de colectare, și apoi elaborează

modalităţi de a le aduce sub privirea vigilentă a agenţiei. Un program aparent obscur demonstrează acest lucru.

Atât NSA, cât și GCHQ au fost extrem de preocupate de necesitatea de a monitoriza comunicaţiile pe internet și telefon ale oamenilor la bordul avioanelor comerciale. Pentru că acestea sunt redirecţionate printr-un sistem de sateliţi independent, ele sunt extrem de dificil de localizat. Ideea că există un moment când cineva poate folosi internetul sau telefonul fără a fi detectat – chiar și pentru câteva ore în timpul zborului – este intolerabilă pentru agenţiile de supraveghere. Ca răspuns, ele au dedicat resurse considerabile pentru a dezvolta sisteme ce vor intercepta comunicaţiile în timpul zborului.

La conferinţa alianţei Five Eyes din 2012, GCHQ a prezentat un program de interceptare denumit Thieving Magpie [Coţofana hoaţă], care urmărește folosirea, tot mai disponibilă, a telefoanelor mobile în timpul zborurilor:





Soluţia propusă are în vedere un sistem pentru a asigura „acoperirea globală“ completă:



S-a făcut un progres substanţial pentru a permite ca unele dispozitive să fie susceptibile la supraveghere în avioanele de pasageri:

GCHQ

Informații GPRS

- În prezent, capabil să producă informații cel puțin pentru telefoanele Blackberry în timpul zborurilor
- Capabil să identifice PIN-uri Blackberry și adrese de e-mail asociate
- Conținut de căutat în bazele de date, neselectat pentru Xkeyscore, sunt disponibile mai multe detalii despre folosirea sa

TOP SECRET//COMINT//REL TO USA, FVEY STRAP1

CONTACT INFORMATION REDACTED

GCHQ

Urmărirea în timpul călătoriei

- Putem confirma că selectorii vizați se îmbarcă în anumite curse aeriene aproape în timp real, permițând echipelor de supraveghere sau arestare să fie activate dinainte
- Dacă folosesc date, putem recupera adrese de e-mail, ID-uri de Facebook, adrese de Skype etc.
- Anumite aeronave pot fi urmărite aproximativ la fiecare două minute în timpul zborului

TOP SECRET//COMINT//REL TO USA, FVEY STRAP1

CONTACT INFORMATION REDACTED

Un document NSA legat de acest subiect și prezentat la aceeași conferință, pentru un program intitulat Homing Pigeon [Porumbelul care se întoarce acasă], descrie eforturile de monitorizare a comunicațiilor în aer. Programul agenției urma să fie coordonat cu GCHQ, iar întregul sistem să fie disponibil grupului Five Eyes.

TOP SECRET//COMINT//REL TO USA, FVEY

(U) DRIVER ANALITIC (CONT.)

❑(S//SI//REL FVEY) Întrebare analitică
Se dă un telefon GSM depistat într-o cursă aeriană cunoscută, care este identitatea probabilă (sau identităţile) a abonatului telefonului (şi viceversa)?
❑(TS//SI//REL FVEY) Procedură propusă
Autocorelarea telefoanelor GSM cu abonaţii observată la două sau mai multe zboruri

TOP SECRET//COMINT//REL TO USA, FVEY

TOP SECRET//COMINT//REL TO USA, FVEY

(U) MERGÂND MAI DEPARTE

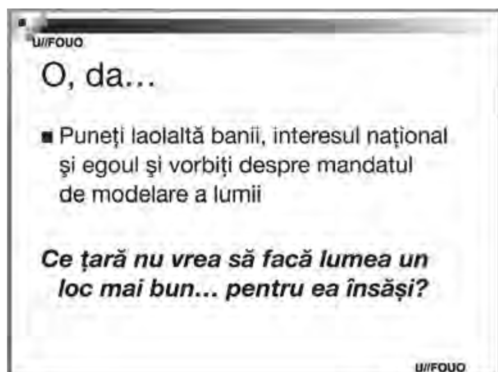
❑ (TS//SI//REL FVEY) SATC va finaliza procesul odată ce a fost stabilit un feed de date THIEVING MAGPIE sigur
❑ (TS//SI//REL FVEY) Odată ce QFD este complet, va fi disponibil pentru utilizatorii FVEY ca serviciu web RESTful, componenta JEMA şi o pagină web light weight
❑ (TS//SI//REL FVEY) Dacă S2 QFD Review Panel alege să ceară ca HOMING PIGEON să fie mai persistent, pagina sa de pornire va fi încorporată în FASTSCOPE

TOP SECRET//COMINT//REL TO USA, FVEY

În unele departamente ale NSA există o sinceritate remarcabilă în legătură cu adevăratul scop al construirii unui sistem de supraveghere atât de masiv. O prezentare în Power Point pregătită pentru un grup de oficiali ai agenţiei care discutau despre perspectiva unor standarde internaţionale pe internet

oferă o imagine necosmetizată. Autorul prezentării este un „ofiţer de informaţii naţionale NSA/SIGINT (SINIO) pentru ştiinţă și tehnologie“, care se autodescrie drept „un om de ştiinţă bine pregătit şi un hacker“.

Titlul acestei prezentări: „Rolul intereselor naţionale, banilor şi egourilor“. Aceşti trei factori împreună, spune el, sunt principalele motive care determină Statele Unite să își păstreze dominaţia în supravegherea globală.



El menţionează că dominaţia SUA asupra internetului a oferit ţării o putere şi o influenţă substanţiale şi a generat un profit enorm:

SECRET//REL TO USA, FVEY

Care este ameninţarea?

- Haideţi să fim sinceri – lumea occidentală (în special SUA) a câştigat influenţă şi a făcut o groază de bani prin schiţarea standardelor timpurii.
  - SUA au fost jucătorul major în modelarea internetului de astăzi. Aceasta a avut ca rezultat exportul generalizat al culturii americane şi al tehnologiei. Faptul a determinat, de asemenea, ca entităţile americane să facă o groază de bani.

Un astfel de profit și o astfel de putere au sporit în mod inevitabil, bineînţeles, industria de supraveghere, furnizând un alt motiv pentru extinderea sa nelimitată. Epoca post 11 septembrie a fost martora unei explozii masive a resurselor dedicate supravegherii. Majoritatea acestor resurse au fost transferate din vistieria publică (contribuabilii americani) în buzunarele unor corporaţii private.

Companii ca Booz Allen Hamilton și AT&T angajează nenumăraţi foști oficiali guvernamentali de rang înalt, în timp ce foarte mulţi actuali oficiali de rang înalt din apărare sunt foști (și probabili viitori) angajaţi ai acelorași corporaţii. Creșterea constantă a supravegherii de stat este o cale de a se asigura că fondurile administraţiei curg, că ușa rotativă rămâne funcţională. Este, de asemenea, cea mai bună modalitate de a se asigura că NSA și agenţiile asociate își menţin importanţa instituţională și influenţa la Washington.

În timp ce scara și ambiţia industriei de supraveghere au crescut, același lucru s-a întâmplat și cu profilul adversarului său. Într-o enumerare a diverselor ameninţări cu care s-ar confrunta Statele Unite, NSA – într-un document intitulat „Agenţia de Securitate Naţională: Informare per ansamblu“ – include unii itemi predictibili: „hackeri“, „elemente infracţionale“ și „teroriști“. În mod revelator totuși, se merge și mai departe incluzându-se printre ameninţări o listă de *tehnologii*, inclusiv internetul:



Internetul a fost multă vreme prezentat ca un instrument de democratizare și liberalizare fără precedent, chiar de emancipare. Dar, în opinia administrației americane, această rețea globală și alte tipuri de tehnologie a comunicațiilor amenință să submineze puterea americană. Privită din această perspectivă, ambiția NSA de a „colecta tot" devine coerentă. Este vital ca NSA să monitorizeze toate componentele internetului și orice alte mijloace de comunicare, astfel ca nimeni să nu scape controlului administrației SUA.

În cele din urmă, dincolo de manipularea diplomatică și câștigul economic, un sistem de spionare omniprezent permite Statelor Unite să își mențină controlul asupra lumii. Când Statele Unite sunt capabile să afle tot ce face, ce spune, ce gândește și ce plănuiește fiecare – propriii săi cetățeni, populația străină, corporațiile internaționale, alți lideri guvernamentali –, puterea sa asupra acestor facțiuni este maximizată. Secretul creează o oglindă cu o singură față: administrația SUA vede ceea ce face oricine altcineva din lume, inclusiv populația sa, în timp ce nimeni nu vede acțiunile sale. Este dezechilibrul ultim, deschizând calea celei mai periculoase dintre condițiile umane: exercitarea unei puteri nelimitate fără transparență sau responsabilitate.

Dezvăluirile lui Edward Snowden au răsturnat acea dinamică periculoasă, scoțând la lumină sistemul și modul în care funcționează acesta. Pentru prima dată, oameni de peste tot au putut să afle adevărata amploare a capacităților de supraveghere mobilizate împotriva lor. Dezvăluirea a generat o dezbatere intensă și susținută la nivel mondial tocmai pentru că supravegherea reprezintă o amenințare gravă la adresa guvernării democratice. Aceasta a generat și propuneri de reformă, o discuție globală despre importanța libertății internetului și a intimității în epoca electronică și o confruntare cu întrebarea vitală: ce înseamnă supravegherea nelimitată pentru noi ca indivizi, în propriile noastre vieți?

Capitolul 4

Răul produs de supraveghere

Guvernele din întreaga lume au făcut încercări energice de a-și antrena cetățenii să desconsidere propria lor intimitate. O litanie de platitudini, de acum familiare, a convins oamenii să tolereze încălcarea severă a vieții lor private; atât de reușite sunt aceste justificări pe care multe persoane le aplaudă, încât autoritățile colectează cantități vaste de date în legătură cu ce spun, ce citesc, ce cumpără acestea – și împreună cu cine.

Aceste autorități statale au fost asistate în asaltul lor asupra vieții private de un cor de moguli ai internetului – indispensabilii parteneri în supraveghere ai administrației. Când directorul general al Google, Eric Schmidt, a fost întrebat în 2009 într-un interviu la CNBC în legătură cu îngrijorările cu privire la reținerea de către compania sa a datelor utilizatorilor, el a replicat în mod scandalos: „Dacă ai ceva despre care nu vrei să știe nimeni, poate nu ar trebui să o faci în primul rând".[1] Cu aceeași desconsiderare, fondatorul și directorul general al Facebook, Mark Zuckerberg, a declarat într-un interviu în 2010 că „oamenii au început să se simtă mai confortabil nu numai partajând mai multe informații și diverse lucruri, ci și fiind mai deschiși cu mai multe persoane".[2] Intimitatea în era digitală nu mai este o „normă socială", a afirmat el, o noțiune care în mod convenabil servește intereselor unei companii de tehnologie care comercializează informații personale.

Dar importanța intimității este evidentă în faptul că până și cei care o devalorizează, care au declarat-o moartă sau dispensabilă, nu cred în ceea ce spun. Militanții antiintimitate au mers foarte departe pentru menținerea controlului asupra vizibilității comportamentului și a informațiilor proprii. Administrația

americană a folosit măsuri extreme pentru a acoperi acţiunile sale de ochii publicului, ridicând un zid care nu a fost niciodată mai înalt, un zid al secretului, în spatele căruia operează. Așa cum arată un raport al ACLU din 2011, „astăzi, mare parte din activitatea administraţiei se desfășoară în secret".[3] Atât de secretoasă este această lume din umbră, „atât de extinsă, de masivă", așa cum afirmă *Washington Post*, „încât nimeni nu știe cât costă, câte persoane angajează, câte programe există în interiorul ei sau câte agenţii fac aceeași muncă". [4]

În mod similar, acei moguli ai internetului care sunt atât de dornici să devalorizeze intimitatea noastră sunt extrem de protectori cu a lor. Google a insistat asupra unei politici de a nu le vorbi reporterilor de la CNET[5], un site de știri din domeniul tehnologiei, după ce CNET a publicat detalii personale despre Eric Schmidt – inclusiv salariul său, donaţiile la campaniile electorale, adresele, toate informaţiile publice obţinute prin intermediul Google – pentru a sublinia pericolele invazive ale companiei sale.

Între timp, Mark Zuckerberg a cumpărat patru case[6] pe lângă cea deţinută în Palo Alto, la un preţ de 30 de milioane de dolari, pentru a-și asigura intimitatea. Așa cum afirma CNET, „viaţa ta personală este cunoscută acum ca date Facebook. Viaţa personală a directorului său general este cunoscută acum ca vezi-ţi de treaba ta".

Aceeași contradicţie este exprimată de mulţi cetăţeni obișnuiţi care desconsideră valoarea intimităţii, dar cu toate acestea au parole la e-mail și la conturile de pe reţelele de socializare. Ei încuie ușa la baie; sigilează plicurile în care își pun scrisorile. Atunci când nimeni nu se uită, adoptă un comportament pe care nu l-ar adopta când sunt la vedere. Ei le spun prietenilor, psihologului și avocaţilor lucruri pe care nu vor să le știe altcineva. Se exprimă online, dar nu vor ca aceste gânduri să fie asociate cu numele lor.

Mulţimea de susţinători ai supravegherii cu care am discutat de la dezvăluirile lui Snowden a împrumutat rapid opinia

lui Eric Schmidt că intimitatea este pentru persoanele care au ceva de ascuns. Dar nici unul dintre ei nu a vrut să îmi dea parola lui de e-mail sau să permită camere de luat vederi în locuinţa sa.

Atunci când președintele Comisiei pentru serviciile de informaţii din Senat, Dianne Feinstein, a insistat că strângerea de metadate de către NSA nu constituie supraveghere – pentru că nu include conţinutul comunicaţiilor –, protestatarii online i-au cerut să își susţină afirmaţiile cu acţiuni: ar publica senatorul în fiecare lună o listă cu toate persoanele cărora le-a trimis e-mailuri sau pe care le-a sunat, inclusiv durata apelului și locul unde se aflau acestea în momentul apelului? Ar fi de neconceput să accepte, tocmai pentru că acest tip de informaţie constituie o adevărată încălcare a vieţii private.

Ceea ce vreau să subliniez nu este ipocrizia celor care discreditează valoarea intimităţii în timp ce o protejează intens pe a lor, deși acest lucru este izbitor. Ci este faptul că dorinţa de intimitate este împărtășită de noi toţi ca esenţială, nu auxiliară, ca fiind o parte din ceea ce înseamnă să fii om. Cu toţii, instinctiv, înţelegem că viaţa privată este acolo unde putem acţiona, gândi, vorbi, scrie, experimenta și alege cum să fim, departe de ochii critici ai altora. Intimitatea este condiţia principală pentru a fi o persoană liberă.

Poate cea mai faimoasă formulare a ceea ce înseamnă intimitatea și a motivului pentru care este ea atât de dorită la nivel universal a fost oferită de judecătorul Curţii Supreme de Justiţie Louis Brandeis în 1928, în cazul *Olmstead v. U.S.*: „Dreptul de a fi singur (este) cel mai cuprinzător dintre drepturi și dreptul cel mai apreciat de o persoană liberă“.[7] Valoarea intimităţii, a scris el, „este mult mai largă ca scop“ decât libertatea civică. Este fundamentală, a spus el:

> Părinții Constituției noastre au încercat să asigure condiții favorabile pentru căutarea fericirii. Ei au recunoscut semnificația naturii spirituale a omului, a sentimentelor şi a intelectului său.

> Ei au ştiut că doar o parte din durere, plăcere şi satisfacţii în viaţă se fundamentează pe drepturi materiale. Au încercat să îi protejeze pe americani în ceea ce priveşte credinţele lor, gândurile, emoţiile şi senzaţiile lor. Ei au conferit, inclusiv împotriva administraţiei, dreptul de a fi lăsat singur.

Chiar înainte de a fi numit la Curtea Supremă, Brandeis a fost un susţinător ardent al importanţei intimităţii. Împreună cu avocatul Samuel Warren, a scris în 1890 în *Harvard Law Review* articolul „Dreptul la intimitate“[8], în care argumenta că să îi răpești cuiva dreptul la intimitate este o infracţiune de o natură profund diferită față de furtul unor bunuri materiale. „Principiul care protejează scrierile personale și toate celelalte producţii personale, nu împotriva furtului și utilizării fizice, ci împotriva publicării sub orice formă, este în realitate nu principiul proprietăţii private, ci acela al personalităţii inviolabile.“

Intimitatea este esenţială pentru libertatea și fericirea umană din motive care sunt discutate rar, dar sunt înţelese instinctiv de majoritatea oamenilor, lucru demonstrat de faptul că aceștia sunt dispuși să meargă atât de departe pentru a o proteja. În primul rând, oamenii își schimbă radical comportamentul atunci când știu că sunt priviţi. Ei se vor strădui să facă tot ce se așteaptă de la ei. Vor să evite rușinea și criticile. Fac acest lucru aderând la practici sociale acceptate, menţinându-se în limitele impuse, evitând acţiuni care ar putea fi văzute ca deviante sau anormale.

Gama de alegeri pe care oamenii le iau în considerare atunci când cred că alţii se uită la ei este totuși mult mai limitată decât atunci când acţionează în intimitate. Negarea intimităţii restricţionează sever libertatea de alegere a cuiva.

În urmă cu câţiva ani am participat la ceremonia de bar mitzvah a celei mai bune prietene a fiicei mele. În timpul ceremoniei, rabinul a subliniat că „lecţia fundamentală“ pe care trebuie să o înveţe o fată este că ea este „privită și judecată

mereu“. I-a spus că Dumnezeu știe întotdeauna ce face, îi știe fiecare alegere, fiecare acţiune și fiecare gând, indiferent cât de intim este acesta. „Nu ești niciodată singură“, a spus el, ceea ce însemna, altfel spus, că ea trebuie să adere întotdeauna la voinţa Domnului.

Ideea rabinului a fost clară: dacă nu poţi evada niciodată de sub privirea atentă a unei autorităţi supreme, nu există altă alegere decât să urmezi dictatele impuse de autoritate. Nu poţi nici măcar să te gândești să îţi creezi propria cale dincolo de aceste reguli: dacă tu crezi că ești întotdeauna privit și judecat, nu ești cu adevărat un individ liber.

Toate autorităţile opresive – politică, religioasă, societală, parentală – se bazează pe acest adevăr vital, folosindu-l ca principal instrument pentru a consolida doctrine, pentru a constrânge la aderare și a anula opinii diferite. Este în interesul lor să comunice că nimic din ce fac supușii lor nu scapă cunoașterii autorităţilor. Mult mai eficientă decât o poliţie, privarea de intimitate va zdrobi orice tentativă de a devia de la reguli și norme.

Ceea ce se pierde atunci când este abolită viaţa privată este mare parte din atributele asociate cu calitatea vieţii. Cele mai multe persoane au trăit senzația că intimitatea le eliberează de constrângere. Și cu toţii am experimentat, pe de altă parte, un comportament privat atunci când am crezut că suntem singuri – dansând, confesându-ne, explorând dorințe sexuale, împărtășind idei –, dar ne-am simţit rușinaţi atunci când am fost văzuţi de alţii.

Doar atunci când credem că nimeni nu se uită la noi ne simţim liberi – în siguranţă – să experimentăm cu adevărat, să testăm limite, să explorăm noi căi de gândire și de existență, să descoperim ceea ce înseamnă să fim noi înșine. Ceea ce a făcut internetul atât de atrăgător a fost exact faptul că îţi permite să vorbești și să acţionezi în anonimat, ceea ce este vital pentru explorarea individuală.

Din acest motiv, pe terenul intimităţii germinează creativitatea, critica și provocările la adresa doctrinei. O societate în care fiecare știe că poate fi privit de stat – în care viaţa privată este efectiv eliminată – este una în care aceste atribute se pierd, atât la nivel societal, cât și individual.

Supravegherea în masă de către stat este, prin urmare, represivă în mod inerent, chiar în cazul improbabil în care nu este folosită abuziv de oficiali răzbunători în scopuri precum obţinerea unor informaţii private despre oponenţii lor politici. Indiferent de cum este folosită supravegherea, limitele pe care aceasta le impune libertăţii sunt intrinsece existenţei sale.

Invocarea cărţii *1984* a lui George Orwell este cumva un clișeu, dar ecourile în legătură cu avertizările sale relativ la supravegherea de stat realizată de NSA sunt clare: amândouă se bazează pe existenţa unui sistem tehnologic care are capacitatea de a monitoriza fiecare acţiune și cuvânt ale cetăţenilor. Similaritatea este negată de campionii supravegherii – noi nu urmărim *mereu*, spun ei –, dar acest argument nu își atinge scopul. În *1984*, cetăţenii nu sunt monitorizaţi neapărat tot timpul; de fapt, ei nu știu dacă sunt monitorizaţi vreodată. Dar statul are capacitatea de a privi tot timpul. Nesiguranţa și posibilitatea unei supravegheri omniprezente sunt cele care îi menţin pe toţi în rând:

> Tele-ecranul recepționează şi transmite simultan. Orice sunet pe care l-ar scoate Winston, mai tare decât o şoaptă foarte slabă, poate fi captat; în plus, atâta timp cât se află în câmpul vizual al plăcii de metal, poate fi şi văzut, nu numai auzit. Sigur că nu ai cum şti, în fiecare moment, dacă eşti sau nu ascultat. Cât de des sau după ce criterii intră Poliția Gândirii pe fiecare post individual este ceva ce ține de domeniul presupunerilor. N-ar fi imposibil nici să urmărească tot timpul pe toată lumea. În tot cazul, pot intra pe firul tău când au ei chef. Te obligă să trăieşti – şi, de fapt, chiar aşa trăieşti, dintr-o obişnuință devenită instinct – cu presupunerea că orice sunet pe care-l

scoți este ascultat şi orice mişcare observată, afară de cazul când, să zicem, stai pe întuneric.*[9]

Chiar și NSA, cu toată capacitatea sa, nu poate citi fiecare e-mail, nu poate asculta fiecare telefon și urmări acţiunile fiecărui individ în parte. Ceea ce face eficient sistemul de supraveghere în controlarea comportamentului uman este să știi că toate cuvintele și acţiunile cuiva sunt susceptibile de monitorizare.

Acest principiu s-a aflat în centrul concepţiei de Panopticon a filosofului britanic din secolul al XVIII-lea Jeremy Bentham, un proiect de clădire despre care el credea că ar permite instituţiilor să controleze eficient comportamentul uman. Structura clădirii urma să fie folosită, potrivit lui, pentru „orice tip de instituţie, în care persoane din toate categoriile sociale urmau să fie ţinute pentru verificare“[10]. Arhitectura iniţială a Panopticonului era un turn central din care fiecare încăpere – sau celulă, sală de clasă sau curte – putea fi monitorizată în orice moment de gardieni. Cu toate acestea, locuitorii nu puteau vedea în turn și astfel nu puteau ști niciodată dacă sunt sau nu supravegheaţi.

De vreme ce instituţia – orice instituţie – nu putea urmări toate persoanele tot timpul, soluţia lui Bentham a fost crearea unei „aparente omniprezenţe a supraveghetorului“ în minţile locuitorilor. „Persoanele care trebuiau supravegheate trebuiau să se simtă întotdeauna ca și cum ar fi fost verificate, cel puţin ca și cum ar fi fost șanse mari să fie.“ Ele ar acţiona astfel ca și cum ar fi priviţi mereu, chiar dacă nu ar fi fost. Rezultatul ar fi ascultarea, obedienţa și conformarea faţă de așteptări. Bentham și-a imaginat că această creaţie se va extinde dincolo de închisori și spitale pentru boli psihice la toate instituţiile societății. El a înţeles că întipărirea în mintea cetăţenilor a faptului că pot fi monitorizaţi mereu revoluţionează comportamentul uman.

* George Orwell, *1984*, Polirom, 2002, trad. Mihnea Gafița

În anii 1970, Michel Foucault a observat că principiul Panopticonului lui Bentham a fost unul dintre mecanismele fundamentale ale statului modern. În *Puterea*, el a scris că panopticonismul este „un tip de putere care este aplicată indivizilor sub forma unei supravegheri individuale continue, sub formă de control, pedeapsă și răsplată și sub formă de corecţie, adică formarea și transformarea individului în termenii acestor norme“.[11]

În *A supraveghea și a pedepsi*, Foucault explică în continuare că supravegherea omniprezentă nu numai că oferă putere autorităţilor și obligă la supunere, ci determină indivizii să interiorizeze faptul că sunt supravegheaţi. Cei care cred că sunt supravegheaţi vor alege în mod instinctiv să facă tot ce se vrea de la ei, fără să își dea seama că sunt controlaţi – Panopticon induce „în deţinut o stare de vizibilitate conștientă și permanentă care asigură funcţionarea automată a puterii“. Odată ce controlul a fost internalizat, dovada evidentă a represiunii dispare pentru că nu mai este necesară: „puterea externă poate renunţa la puterea sa fizică; ea tinde să fie non-corporală; și, cu cât se apropie mai mult de această limită, cu atât efectele sale sunt mai constante, mai profunde și permanente: este o victorie profundă care evită orice confruntare fizică și care este întotdeauna decisă dinainte“.

În plus, acest tip de control are marele avantaj al creării simultane a iluziei de libertate. Constrângerea la supunere există în mintea individului. Indivizii aleg de bunăvoie să se supună, de teama că sunt supravegheaţi. Aceasta elimină nevoia tututor semnelor de constrângere și astfel permite controlul asupra persoanelor care cred în mod fals că sunt libere.

Din acest motiv, orice stat opresiv vede supravegherea în masă ca fiind unul dintre cele mai vitale instrumente de control. Când cancelarul german Angela Merkel, de obicei reţinută în declaraţii, a aflat că NSA a petrecut ani întregi ascultându-i telefonul personal, a vorbit cu președintele Obama și a comparat furioasă supravegherea SUA cu cea a STASI[12], cunoscutul

serviciu de securitate din Germania de Est, unde a crescut. Merkel nu a vrut să spună că Statele Unite sunt echivalente cu regimul comunist, ci mai degrabă că esenţa unui stat supraveghetor ameninţător, fie că este NSA sau STASI sau Big Brother (Fratele cel Mare) sau Panopticon, este să știi că cineva este supravegheat în orice moment de autorităţi nevăzute.

Nu este greu de înţeles de ce autorităţile din Statele Unite și din alte ţări occidentale au încercat să construiască un sistem omniprezent de spionare îndreptat împotriva propriilor cetăţeni. Inegalităţile economice tot mai mari, agravate de colapsul financiar din 2008, au generat o instabilitate internă gravă. Au fost revolte vizibile chiar și în democraţiile relativ stabile, precum Spania și Grecia. În 2011 au fost zile de revolte la Londra. În Statele Unite, atât dreapta – protestele Tea Party din 2008 și 2009 –, cât și stânga – mișcarea Occupy – au lansat proteste cetăţenești de durată. Sondajele în aceste ţări au arătat un nivel izbitor de intens de nemulţumire faţă de clasa politică și direcţia înspre care se îndreaptă societatea.

Autorităţile confruntate cu o revoltă au, în general, două opţiuni: să împace populaţia cu concesii simbolice sau să își intensifice controlul pentru a minimiza prejudiciul pe care aceasta îl poate crea intereselor sale. Elitele din Occident par să vadă a doua opţiune – consolidarea puterii – ca fiind mai bună, poate singurul curs viabil al acţiunii pentru a-și proteja poziţia. Răspunsul faţă de mișcarea Occupy a fost zdrobirea ei prin forţă, cu gaze lacrimogene, spray paralizant și urmărire penală. Paramilitarizarea forţelor de poliţie interne a fost etalată complet în orașele americane, în timp ce ofiţerii de poliţie au adus arme văzute pe străzile din Bagdad pentru a înăbuși protestatarii reuniţi legal și în mare măsură pașnici. Strategia a fost ca oamenilor să le fie indusă frica de a participa la marșuri și proteste, iar acest lucru a funcţionat, în general. Scopul mai general a fost cultivarea sentimentului că acest tip

de rezistență este inutil împotriva unei forțe instituționale masive și impenetrabile.

Un sistem de supraveghere omniprezentă ascunde același scop, dar cu o potențialitate chiar și mai mare. Simpla organizare a mișcărilor de contestare devine dificilă când administrația urmărește ce face fiecare persoană. Dar supravegherea în masă ucide contestarea într-un mod și mai profund și mult mai important: în minte, acolo unde individul se antrenează să gândească doar în conformitate cu ce se așteaptă și se cere de la el sau ea.

Istoria nu lasă nici o urmă de îndoială privitor la faptul că atât constrângerea colectivă, cât și controlul reprezintă în același timp intenția și efectul supravegherii statului. Scenaristul de la Hollywood Walter Bernstein, care s-a aflat pe lista neagră și a fost monitorizat în perioada lui McCarthy,[13] fiind obligat să scrie sub pseudonim pentru a-și putea continua activitatea, a descris o dinamică a autocenzurării opresive care vine din sentimentul că ești supravegheat:

> Toată lumea era atentă. Nu era momentul pentru discuții riscante... Au fost scriitori, nu scriitori aflați pe lista neagră, care au făcut, nu știu cum le-ați spune, „lucruri inovatoare“, dar nu politice. Au stat departe de politică... Cred că era un sentiment general de „nu îți asumi riscuri“.
>
> Nu este o atmosferă care să ajute creativitatea sau care să lase mintea să cutreiere liberă. Ești permanent în pericolul de a te autocenzura, de a spune „nu, nu voi încerca acest lucru pentru că știu că nu se va concretiza sau va îndepărta guvernul“ sau ceva de genul acesta.

Observațiile lui Bernstein au avut ecou într-un raport[14] publicat de PEN America în noiembrie 2013, intitulat *Consecințe descurajante: Supravegherea NSA împinge scriitorii americani la autocenzură*. Organizația a realizat un sondaj pentru a urmări efectele dezvăluirilor privind NSA asupra membrilor săi, ajungând la concluzia că mulți scriitori „își asumă acum că le

sunt monitorizate comunicaţiile" şi şi-au schimbat comportamentul în moduri care „le reduc libertatea de exprimare şi le restricţionează fluxul liber de informaţii". Mai exact, „24% au evitat în mod deliberat anumite teme în conversaţiile telefonice sau pe e-mail".

Puterea de control pernicioasă a supravegherii omniprezente şi autocenzurarea care rezultă sunt confirmate printr-o gamă largă de experimente sociale şi se extind dincolo de activismul politic. Studii ample arată cum funcţionează această dinamică la cel mai profund nivel personal şi psihologic.

O echipă de cercetători[15], care şi-a publicat descoperirile în revista *Evolutionary Psychology*, le-a prezentat subiecţilor lor acţiuni morale discutabile,precum păstrarea unei cantităţi considerabile de bani găsită într-un portofel pe stradă sau cunoaşterea faptului că un prieten a introdus informaţii false în CV-ul său. Subiecţii au fost rugaţi să evalueze gradul de infracţionalitate. Studiul a menţionat că subiecţii cărora le-au fost arătate imagini care sugerează supravegherea, precum o pereche de ochi mari care îi fixează, au calificat acţiunile ca fiind mai „reprobabile" decât cei cărora le-a fost arătată o imagine neutră. Cercetătorii au conchis că supravegherea îi încurajează pe cei care sunt urmăriţi să „îşi afirme susţinerea faţă de normele sociale prevalente" în timp ce încearcă să „îşi gestioneze activ reputaţia".

Un experiment cuprinzător desfăşurat în 1975[16] de psihologii Gregory White şi Philip Zimbardo de la Universitatea Standford, intitulat „Consecinţele descurajante ale supravegherii", a intenţionat să evalueze dacă să fii supravegheat are vreun impact asupra exprimării unor opinii politice controversate. Impulsul de la care a pornit studiul au fost îngrijorările americanilor legate de supravegherea de către administraţie.

> Scandalul Watergate, dezvăluirile cu privire la ascultarea cu microfoane de către Casa Albă şi investigaţiile Congresului asupra spionajului intern desfăşurat de Agenţia Centrală de Informaţii

> au servit la amplificarea temei paranoide a vieții americane: Fratele cel Mare poate că te supraveghează! Propunerile de bănci de date naționale, folosirea elicopterelor de supraveghere de către forțele de poliție orăşeneşti, prezența camerelor de supraveghere în bănci şi supermarketuri şi controalele de securitate din aeroport asupra persoanei şi bunurilor sale sunt doar câteva dintre semnele că viețile noastre private se află sub o astfel de supraveghere tot mai mare.

Participanţii au fost plasaţi sub niveluri diferite de supraveghere și li s-a cerut să își spună opiniile despre legalizarea marijuanei.

A reieșit că subiecţii „amenințaţi" – cei cărora li s-a spus că declaraţiile lor vor fi împărtășite poliţiei „în scopuri educaţionale" – au fost mai înclinaţi să condamne folosirea marijuanei și să întrebuințeze pronumele la persoana a doua sau a treia („voi", „ei", „oamenii") în limbaj. Doar 44% dintre subiecţii aflaţi sub supraveghere au susţinut legalizarea, comparativ cu 77% dintre cei care nu erau atât de „amenințaţi". Practic, 31% dintre participanţii monitorizaţi spontan au căutat aprobarea cercetătorilor (întrebând, de exemplu, „Este corect?"), în timp ce doar 7% din celălalt grup au făcut acest lucru. Participanţii care erau „amenințaţi" au înregistrat scoruri semnificativ mai mari în ceea ce privește anxietatea și inhibiţia.

White și Zimbardo au notat în concluzie că „amenințarea sau exercitarea supravegherii guvernamentale poate inhiba psihologic libertatea de exprimare". Ei au adăugat că, în timp ce „modul în care a fost conceput studiul lor nu a dat posibilitatea de a «evita reuniunea»", se așteaptă ca „anxietatea generată de amenințarea supravegherii să determine multe persoane să evite total situaţiile" în care ar putea fi monitorizate. „De vreme ce aceste presupuneri sunt limitate doar de imaginaţie și sunt încurajate zilnic de dezvăluiri privind invadarea intimităţii de către administraţie și instituţii", au scris ei, „limitele

dintre delirul paranoid și precauţia justificată devin într-adevăr tot mai fragile".

Este adevărat că supravegherea poate uneori să promoveze ceea ce unii ar putea considera un comportament dezirabil. Un studiu[17] consideră că tulburările de pe stadioanele de fotbal suedeze – microbiști care aruncă cu sticle și brichete pe teren – au scăzut cu 65% după introducerea camerelor de supraveghere. Iar literatura din domeniul sănătăţii publice cu privire la spălatul pe mâini[18] a confirmat în mod repetat că modul de a crește probabilitatea ca un om să se spele pe mâini este să pui pe altcineva în apropiere.

Dar, în mod covârșitor, efectul de a fi supravegheat constrânge prea sever alegerea individuală. Chiar și în cele mai intime cadre, în familie, de exemplu, supravegherea transformă acţiuni nesemnificative într-o sursă de autojudecare și anxietate, doar prin simplul fapt de a fi urmărit. Într-un experiment[19] din Marea Britanie, cercetătorii au furnizat subiecţilor dispozitive de urmărire pentru a ţine sub observaţie membrii familiei. Locul exact al fiecărui membru al familiei era accesibil în orice moment și, dacă locul în care se afla cineva era văzut, persoana urmărită primea un mesaj. De fiecare dată când un membru al familiei îl urmărea pe altul, i se cerea să completeze un chestionar în care era întrebat de ce a făcut acest lucru și dacă informaţiile primite se potriveau așteptărilor sale.

Pe durata interviurilor, participanţii au declarat că uneori considerau urmărirea reconfortantă, dar se simţeau neliniștiţi pentru că, dacă se aflau într-un loc neașteptat, membrii familiei s-ar fi putut „grăbi să tragă concluzii" despre comportamentul lor. Iar opţiunea de a „deveni invizibil" – prin blocarea mecanismului de partajare a localizării – nu îndepărta neliniștea: mulţi participanţi au declarat că actul de a evita supravegherea în sine ar genera suspiciune. Cercetătorii au conchis:

> Sunt trasee în viaţa noastră de zi cu zi pe care nu le putem explica şi care ar putea fi complet nesemnificative. Totuşi,

> reprezentarea lor printr-un dispozitiv de urmărire... le conferă semnificație, generând un grad extraordinar de responsabilitate. Aceasta produce nelinişte, mai ales în cadrul relațiilor apropiate, în care oamenii resimt o mare presiune să dea socoteală pentru lucruri de care pur şi simplu nu sunt responsabili.

Potrivit unui experiment finlandez care a întreprins una dintre cele mai radicale simulări ale supravegherii[20], au fost amplasate camere de luat vederi în casele subiecţilor – cu excepţia băilor și a dormitoarelor – și toate comunicaţiile lor electronice au fost urmărite. Deși publicitatea făcută studiului a devenit virală pe reţelele de socializare, cercetătorii au avut dificultăţi în a găsi măcar zece locuinţe care să participe.

Printre cei care s-au înscris, plângerile legate de proiect s-au concentrat pe invadarea unor părţi obișnuite din vieţile lor cotidiene. O persoană s-a simţit inconfortabil să fie goală în propria casă; alta a conștientizat prezenţa camerelor în timp ce își aranja părul după duș; o altă persoană s-a gândit la supraveghere în timp ce își injecta medicamentele. Acţiuni inofensive au căpătat semnificaţie atunci când au fost supravegheate.

Subiecţii au descris iniţial supravegherea ca plictisitoare; totuși, curând, „s-au obișnuit cu ea". Ceea ce a început ca o invadare profundă a devenit ceva normal, s-a transformat într-o situaţie obișnuită și nu a mai fost remarcată.

Așa cum arată experimentul, există tot felul de lucruri pe care oamenii le fac și pe care vor să le păstreze pentru ei, chiar dacă aceste lucruri nu reprezintă „ceva rău". Intimitatea este indispensabilă unei game extinse de activităţi umane. Dacă cineva sună la o linie telefonică pentru sinucigași sau vizitează o clinică pentru avorturi sau este tratat de o boală, sau dacă un avertizor de integritate sună un reporter, sunt multe motive de a păstra aceste acte private, care nu au legătură cu vreo ilegalitate sau infracţiune.

Pe scurt, toată lumea are ceva de ascuns. Reporterul Barton Gellman[21] a tras următoarea concluzie:

> Intimitatea este relațională. Depinde de publicul pe care îl ai. Nu vrei ca angajatorul tău să ştie că eşti la vânătoare de locuri de muncă. Nu le spui totul despre viața ta amoroasă mamei tale sau copiilor tăi. Nu dezvălui secrete comerciale rivalilor tăi. Nu ne expunem fără discriminare şi ne pasă suficient de expunere pentru a minți automat. În rândul cetățenilor respectabili, cercetătorii au descoperit că minciuna este „o interacțiune socială zilnică“ (de două ori pe zi în rândul studenților, o dată pe zi în Lumea Reală)... Transparența completă este un coşmar... Toată lumea are ceva de ascuns.

O justificare esenţială a supravegherii – că este în beneficiul populaţiei – se bazează pe proiectarea unei viziuni despre lume care împarte cetăţenii în oameni buni și oameni răi. În această viziune, autorităţile își folosesc puterile de supraveghere împotriva oamenilor răi, a acelora care „fac ceva rău“ și doar ei trebuie să se teamă de invadarea intimităţii. Aceasta este o tactică veche. Într-un articol din 1969 al revistei *Time* despre îngrijorările tot mai mari ale americanilor în legătură cu puterile de supraveghere guvernamentale, procurorul general al lui Nixon, John Mitchell, asigura cititorii că „orice cetăţean al Statele Unite care nu este implicat în vreo activitate ilegală nu are de ce să se teamă“.[22]

Ideea a fost reluată de un purtător de cuvânt al Casei Albe, care a răspuns în 2005 unei controverse privind programul de supraveghere ilegală al lui Bush: „Nu este vorba despre monitorizarea apelurilor telefonice legate de antrenamentul în Little League sau a celor privitoare la ce să aduci la o cină între prieteni. Acestea urmăresc să monitorizeze apelurile oamenilor răi către alţi oameni răi“.[23] Iar atunci când președintele Obama a apărut la *The Tonight Show*[24] în august 2013 și a fost întrebat de Jay Leno despre dezvăluirile NSA, el a spus: „Nu avem un program de spionaj intern. Avem unele mecanisme care pot urmări un număr de telefon sau o adresă de e-mail care este legată de un atac terorist“.

Pentru mulţi, argumentul funcţionează. Percepţia că această supraveghere invazivă este limitată doar la un grup marginal și care merită acest lucru, de „răufăcători“ – oamenii răi –, asigură acceptarea de către majoritate a abuzului de putere sau chiar lăudarea lui.

Dar această percepţie pierde din vedere în mod radical ce scopuri motivează toate instituţiile autorităţii. „Să faci ceva rău“ în concepţia unor astfel de instituţii depășește cu mult actele ilegale, comportamentul violent și comploturile teroriste. Acest lucru se extinde de obicei la contestarea semnificativă și la orice provocare nevinovată. Stă în natura autorităţii să echivaleze contestarea cu faptele rele sau cel puţin cu o ameninţare.

Există numeroase exemple de grupuri și de indivizi care au fost plasaţi sub supraveghere guvernamentală în virtutea vederilor lor contestatare sau a activismului – Martin Luther King, mișcarea pentru drepturile civile, activiștii antirăzboi, ecologiștii. În opinia administraţiei și a directorului FBI J. Edgar Hoover, aceștia „făceau ceva rău“: activitate politică prin care se ameninţa ordinea existentă.

Nimeni nu a înţeles mai bine decât Hoover puterea supravegherii pentru zdrobirea disidenţei politice, în timp ce se confrunta cu provocarea de a preveni exercitarea drepturilor la exprimare și la asociere prevăzute de Primul Amendament atunci când statul este îngrădit în a aresta persoanele care exprimă opinii nepopulare. Anii 1960 au introdus în serie la Curtea Supremă cazuri care au stabilit norme de protecţie riguroase pentru libertatea de exprimare, culminând cu decizia unanimă din 1969 în *Brandenburg v. Ohio*,[25] care a anulat condamnarea penală a unui lider al Ku Klux Klan care ameninţase cu violenţa oficiali politici într-un discurs. Curtea a afirmat că garanţiile din Primul Amendament pentru libertatea de exprimare și presa liberă sunt atât de puternice încât „nu permit statului să interzică sau să scoată în afara legii militantismul pentru folosirea forţei“.

Având în vedere aceste garanţii, Hoover a instituit un sistem pentru a preveni în primul rând dezvoltarea contestării.

Programul de contraspionaj intern al FBI, COINTELPRO, a fost pentru prima dată dezvăluit de un grup de activiști antirăzboi convinși că se făcuseră infiltrări în mișcarea antirăzboi, că aceasta fusese pusă sub supraveghere și vizată de tot felul de lucruri murdare. Neavând probe pentru a dovedi acest lucru și nereușind să convingă jurnaliștii să scrie despre suspiciunea lor, ei au pătruns într-un birou al FBI din Pennsylvania în 1971 și au luat mii de documente.

Documentele legate de COINTELPRO au arătat cum a urmărit FBI grupuri politice și indivizi pe care îi considera subversivi și periculoși, inclusiv Asociaţia Naţională pentru Progresul Persoanelor de Culoare, mișcări naţionaliste ale persoanelor de culoare, organizaţii socialiste și comuniste, protestatari antirăzboi și diverse grupuri de dreapta. Biroul infiltrase agenţi în aceste mișcări care, între altele, încercau să își manipuleze membrii astfel încât aceștia să accepte să comită acte penale pentru ca FBI să îi aresteze și să îi urmărească în justiţie.

FBI a reușit să convingă *New York Times* să interzică tipărirea unor documente și chiar să le returneze, dar *Washington Post* a publicat o serie de articole pe baza lor. Aceste dezvăluiri au condus la crearea Comisiei Church în Senat[26], care a conchis:

> [În decursul a 15 ani] Biroul a desfăşurat o operațiune sofisticată şi vigilentă menită în mod direct să prevină exercitarea drepturilor la libertatea de exprimare şi asociere prevăzute în Primul Amendament, pe baza ipotezei că prevenirea dezvoltării unor grupuri periculoase şi a propagării unor idei periculoase ar proteja securitatea națională şi ar descuraja violența.
>
> Multe dintre tehnicile folosite ar fi intolerabile într-o societate democratică chiar dacă toate țintele ar fi implicate în activități violente, dar COINTELPRO a mers mult mai departe decât atât. Premisa majoră neexprimată a programului a fost că o agenție de aplicare a legii are datoria de a face orice este

necesar pentru a lupta împotriva a ceea ce percepe ca fiind amenințări la adresa ordinii sociale şi politice existente.

Un memorandum cheie[27] al COINTELPRO a explicat că „paranoia" poate fi sădită în rândul activiștilor antirăzboi făcându-i să creadă că există „un agent FBI în spatele fiecărei cutii poștale". Astfel, disidenţii, convinși permanent că sunt supravegheaţi, vor ceda fricii și se vor abţine de la activism.

După cum era de așteptat, tactica a funcţionat. Într-un documentar din 2013[28] intitulat *1971*, câţiva activiști au descris modul în care FBI-ul lui Hoover era prezent „peste tot" în mișcarea pentru drepturi civile cu agenţi infiltraţi și supraveghere, oameni care veneau la întâlnire și apoi raportau. Monitorizarea a stânjenit capacitatea mișcării de a se organiza și de a se dezvolta.

La momentul respectiv, cele mai renumite instituţii din Washington au înţeles că simpla existenţă a supravegherii guvernamentale, indiferent cum este folosită ea, asfixiază capacitatea de contestare. *Washington Post*, într-un editorial din martie 1975 despre spargere, a avertizat tocmai în legătură cu această dinamică opresivă:

> FBI nu a arătat niciodată prea multă sensibilitate față de efectul otrăvitor pe care supravegherea sa şi în special folosirea unor informatori fără chip îl are asupra procesului democratic şi asupra libertății de exprimare. Dar ar trebui să fie evident că discuția şi controversa privind politicile şi programele guvernamentale sunt menite să fie inhibate dacă se ştie că Fratele cel Mare, deghizat, îi ascultă şi îi raportează.[29]

COINTELPRO a fost departe de a fi singurul abuz al supravegherii descoperit de Comisia Church. Raportul său final a declarat că „milioane de telegrame private trimise din sau prin Statele Unite au fost obţinute de Agenţia pentru Securitate Naţională din 1947 și până în 1975, în conformitate cu un aranjament secret cu trei companii de telegrafie din Statele

Unite". Mai mult, „aproximativ 300 000 de persoane au fost indexate într-un sistem computerizat al CIA și au fost create dosare separate pentru aproximativ 7 200 de americani și peste 100 de grupuri interne" în timpul unei singure operaţiuni a CIA, CHAOS (1967–1973).

În plus, „un număr estimat de 100 000 de americani au fost subiecții unor dosare ale Armatei Statelor Unite create între mijlocul anilor 1960 și 1971", iar aproximativ 11 000 de indivizi și grupuri au fost investigaţi de Direcţia Finanţelor Publice (IRS) „pe baza unor criterii mai degrabă politice decât referitoare la impozite". Biroul a folosit, de asemenea, interceptarea pentru a descoperi vulnerabilităţi, precum activitatea sexuală, care erau folosite apoi pentru „neutralizarea" ţintelor sale.

Aceste incidente nu au fost aberaţii ale epocii respective. În timpul lui Bush, de exemplu, documente obţinute[30] de ACLU au dezvăluit, așa cum a arătat grupul în 2006, „noi detalii despre supravegherea desfășurată de Pentagon asupra americanilor care se opuneau războiului din Irak, inclusiv quakeri și grupuri de studenţi". Pentagonul a „ţinut sub observaţie protestatari non-violenţi colectând informaţii și stocându-le într-o bază de date militară antiterorism". ACLU a menţionat că un document, „etichetat ca «activitate potenţial teroristă» listează cazuri precum mitingul «Opriţi războiul ACUM!» din Akron, Ohio".

Dovezile arată că asigurările că supravegherea este îndreptată doar împotriva acelora care „au făcut ceva rău" ar trebui să ofere prea puţină alinare, de vreme ce statul vede în mod reflex orice provocare la adresa puterii sale drept o faptă rea.

Oportunitatea pe care cei de la putere o au de a caracteriza oponenţii politici ca „ameninţări la adresa securităţii naţionale" sau chiar „teroriști" s-a dovedit în mod repetat irezistibilă. În ultimul deceniu, administraţia, ca un ecou la FBI-ul lui Hoover, a desemnat oficial în acest fel activiști ecologiști, serii

întregi de grupări antiguvernamentale de dreapta, activiști antirăzboi și asociații organizate în jurul drepturilor palestiniene. Unii indivizi din cadrul acestor categorii extinse ar putea merita această desemnare, dar indubitabil majoritatea nu o merită, fiind vinovaţi doar de faptul că au vederi politice opuse. În continuare astfel de grupări sunt alese în mod curent ca ţinte ale supravegherii NSA și a partenerilor săi.

Într-adevăr, după ce autorităţile britanice l-au reţinut pe partenerul meu, David Miranda, pe aeroportul Heathrow în conformitate cu o lege antiterorism, guvernul britanic a echivalat în mod expres relatările mele despre supraveghere cu terorismul pe baza faptului că publicarea documentelor lui Snowden „este menită să influenţeze un guvern și este făcută în scopul de a promova o cauză politică sau ideologică. Prin urmare, aceasta intră sub incidenţa definiţiei terorismului". Aceasta este cea mai clară declaraţie posibilă de legare de terorism a unei ameninţări la adresa intereselor puterii.

Nimic din toate acestea nu a constituit o surpriză pentru comunitatea musulmană americană, unde teama de supraveghere în baza terorismului este intensă și universală, și pe bună dreptate. În 2012, Adam Goldman și Matt Apuzzo de la Associated Press au dezvăluit o schemă comună CIA/ Departamentul de poliţie din New York de a supune întreaga comunitate de musulmani din Statele Unite unei supravegheri fizice și electronice fără cea mai mică sugestie de infracţiune. Musulmanii americani descriu în mod obișnuit efectul spionajului asupra vieţilor lor[31]: fiecare persoană nouă care apare la o moschee este privită cu suspiciune ca un informator al FBI; prietenii și familia își limitează discuţiile de teama de a nu fi monitorizaţi și conștientizând faptul că orice opinie exprimată considerată ostilă Americii poate fi folosită ca pretext pentru o investigaţie sau chiar pentru o urmărire judiciară.

Un document din dosarele lui Snowden, datat 3 octombrie 2012, subliniază rece acest punct. Acesta dezvăluie că agenţia a monitorizat activităţile online ale unor persoane despre care

credea că exprimă idei „radicale“ și care au o influenţă „de radicalizare“ asupra altora. Documentul vorbește în special despre șase indivizi, cu toţii musulmani, deși susţine că sunt pur și simplu „exemple“.

NSA afirmă explicit că nici unul dintre indivizii vizaţi nu este membru al unei organizaţii teroriste sau implicat în vreun complot terorist. În schimb, infracţiunea de care se fac vinovaţi ei este reprezentată de vederile pe care le exprimă, considerate „radicale“, un termen care garantează supravegherea universală și campanii distructive pentru „exploatarea vulnerabilităţilor“.

Printre informaţiile colectate despre acești indivizi, dintre care cel puţin unul este american, se numără detalii despre activităţile lor sexuale online și „promiscuitatea online“ – site-uri pornografice pe care le vizitează și discuţii obscure cu caracter sexual cu femei care nu sunt soţiile lor. Agenţia discută modalităţile de a exploata aceste informaţii pentru a le distruge reputaţia și credibilitatea.

TRECUT (U)

(TS//SI//REL TO USA, FVEY) Un raport de evaluare SIGINT anterior despre radicalizare arată că radicalizatorii par să fie deosebit de vulnerabili în zona autorităţii atunci când există diferenţe între comportamentul privat şi cel public. (A) Unele vulnerabilităţi, dacă ar fi expuse, ar arunca îndoială asupra devotamentului radicalizatorului faţă de cauza jihadistă, conducând la degradarea sau pierderea autorităţii sale. Exemple de astfel de vulnerabilităţi sunt:

• vizionarea de materiale online cu caracter sexual explicit sau folosirea unui limbaj sexual explicit convingător atunci când comunică cu tinere fără experienţă;
• folosirea unei părţi a donaţiilor pe care le primesc din partea grupului susceptibil pentru a plăti cheltuieli personale;
• încasarea unei sume de bani exorbitante pentru discursuri şi faptul că sunt atraşi doar de oportunităţile de a-şi creşte reputaţia
• faptul că sunt cunoscuţi pentru că îşi bazează mesajul public pe surse discutabile sau că folosesc un limbaj care este contradictoriu prin natura sa, lăsându-i descoperiţi în faţa provocărilor privind credibilitatea.

(TS//SI// REL TO USA, FVEY) Chestiunile de încredere şi reputaţie sunt importante atunci când se are în vedere validitatea şi atracţia mesajului. Pare rezonabil că exploatarea vulnerabilităţilor de caracter, credibilitate sau ambele, ale radicalizatorului şi mesajului său poate fi intensificată prin înţelegerea mijloacelor pe care le foloseşte pentru a-şi propaga mesajul în grupul susceptibil şi unde este vulnerabil în termeni de acces.

Așa cum a remarcat directorul juridic adjunct al ACLU, Jameel Jaffer, baza de date a NSA „stochează informaţii despre opiniile politice, istoricul medical, relaţiile intime și

activitățile online" ale oamenilor[32]. Agenția pretinde că aceste informații personale nu vor fi folosite abuziv, „dar documentele arată că NSA definește probabil «abuzul» într-un sens foarte restrâns". Așa cum subliniază Jaffer, NSA a folosit în trecut, la solicitarea președinților, „rezultatele supravegherii pentru a discredita un oponent politic, un jurnalist sau un activist pentru drepturile omului". Ar fi „naiv", a spus el, să se creadă că agenția nu își poate „folosi puterea în acest fel".

Alte documente descriu concentrarea administrației nu numai asupra WikiLeaks și a fondatorului său, Julian Assange, ci și asupra a ceea ce agenția numește „rețeaua umană care sprijină WikiLeaks". În august 2010, administrația Obama a cerut câtorva aliați să intenteze acuzații penale împotriva lui Assange pentru publicarea de către grup a jurnalelor de război din Afghanistan. Discuția cu privire la presiunea exercitată asupra altor țări pentru a-l acuza pe Assange apare într-un dosar NSA pe care agenția îl numește „Cronologia vânătorii de oameni". Acesta detaliază, țară după țară, eforturile depuse de Statele Unite și de aliații săi pentru a localiza, urmări judiciar, captura și/sau ucide diverși indivizi, între care presupuși teroriști, traficanți de droguri și lideri palestinieni. Există o cronologie pentru fiecare an între 2008 și 2012.

Un document separat conține un rezumat al schimbului de mesaje din iulie 2011 care analizează dacă WikiLeaks, precum și website-ul de partajare de fișiere Pirate Bay pot fi desemnate cu sintagma „«actor străin rău-intenționat» pentru a fi urmărite". Etichetarea ar permite o supraveghere electronică extinsă asupra acestor site-uri, inclusiv a utilizatorilor americani. Discuția apare într-o listă de „Întrebări și Răspunsuri" în care oficiali din cadrul Biroului de Supraveghere și Conformitate (NOC) al NTOC și Biroului Consiliului General (OGC) al NSA oferă răspunsuri la întrebările adresate.

Un astfel de schimb de mesaje arată indiferența NSA față de încălcarea normelor privind supravegherea. În document, un operator afirmă „am dat-o-n bară", pentru că a urmărit un

cetăţean american în loc de un străin. Răspunsul biroului de supraveghere al NSA și al consiliului general este, „nu ai de ce să îţi faci griji“.

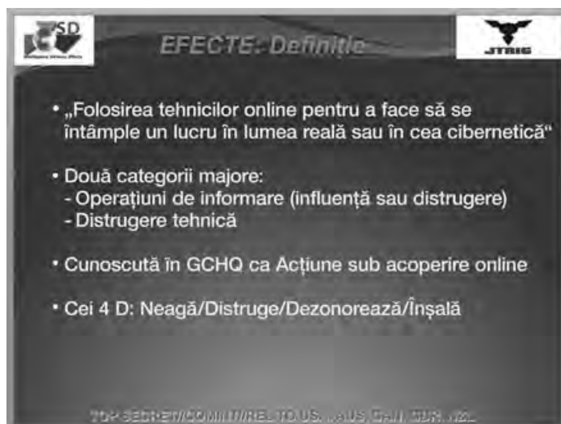
Tratamentul rezervat pentru Anonymous, precum și categoriei vagi de persoane denumite „hacktiviști“, este deosebit de tulburător și extrem. Aceasta pentru că Anonymous nu este un grup structurat, ci o afiliere de persoane în jurul unei idei organizate liber: aceasta poate însemna folosirea unor competenţe în programare pentru a submina securitatea și funcţionarea internetului, dar se poate referi și la oricine folosește instrumente online pentru a promova idei politice. Faptul că NSA vizează astfel de categorii largi de persoane este echivalent cu permiterea spionării oriunde, inclusiv în Statele Unite, a oricui are idei pe care administraţia le consideră ameninţătoare.

Gabriella Coleman, specialistă în Anonymous la Universitatea McGill, a declarat că grupul nu este o „entitate definită“, ci mai degrabă „o idee care mobilizează activiștii să ia atitudine în mod colectiv și să exprime nemulţumirea politică. Este o mișcare socială la nivel global fără o structură de leadership centralizată sau oficială organizată. Unii s-au raliat în jurul numelui pentru a se angaja într-o nesupunere civică digitală, dar nimic nu seamănă nici pe departe a terorism“. Majoritatea celor care au îmbrăţișat ideea au făcut acest lucru „în primul rând pentru exprimare politică obișnuită. Să vizezi Anonymous și hacktiviștii este același lucru cu urmărirea cetăţenilor pentru că își exprimă credinţele politice, rezultând în înăbușirea contestării legitime“, a explicat Coleman.

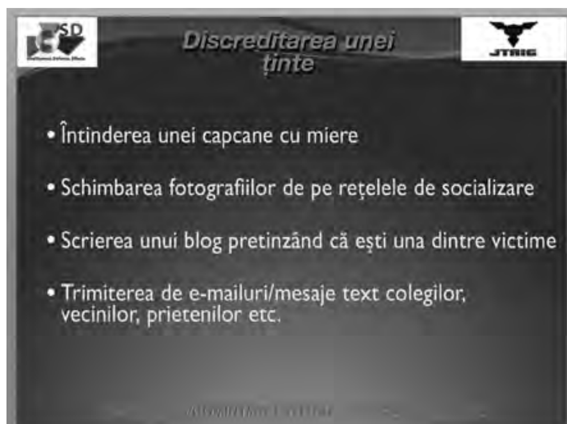
Anonymous a fost ținta unei unități a GCHQ care folosește unele dintre cele mai controversate și radicale tactici cunoscute de spionaj: „operaţiuni sub acoperire“, „capcane cu miere“ *(honey-traps)*, virusuri și alte atacuri, strategii de înșelăciune și „operaţiuni de informare pentru distrugerea reputaţiilor“.

Un slide PowerPoint prezentat de oficialii care se ocupă de supraveghere în GCHQ la conferinţa SigDev din 2012 descrie două forme de atac: „operaţiuni de informare (influenţă sau

distrugere)“ și „distrugere tehnică“. GCHQ se referă la aceste măsuri ca la „Acţiuni sub acoperire online“ menite să obţină ceea ce documentul numește „The 4 D’s: Deny/Disrupt/Degrade/Deceive“ (Cei 4 D: Neagă/Distruge/Dezonorează/Înșală).



Un alt slide descrie tacticile folosite pentru „discreditarea ţintei“. Acestea includ „întinderea unei capcane cu miere“, „schimbarea fotografiilor de pe reţelele de socializare“, „scrierea unui blog pretinzând că ești una dintre victime“ și „trimiterea de e-mailuri/mesaje text colegilor, vecinilor, prietenilor etc.“



În notele care însoţesc prezentarea, GCHQ explică faptul că aceate „capcane cu miere" – o tactică veche din Războiul Rece care presupune folosirea unor femei atractive pentru a ademeni ţinte masculine în situaţii compromiţătoare și care discreditează – au fost adaptate erei digitale: acum o ţintă este ademenită pe un site compromiţător sau la o întâlnire online. Comentariul adaugă: „o opţiune grozavă. Foarte de succes atunci când funcţionează". În mod similar, metode tradiţionale de infiltrare se desfășoară acum online.

O altă tehnică presupune oprirea „cuiva de la a comunica". Pentru a face acest lucru, agenţia va „bombarda telefonul acestuia cu mesaje text", „îi va bombarda telefonul cu apeluri", „îi va șterge prezenţa online" și „îi va bloca faxul".



GCHQ preferă, de asemenea, să folosească tehnici de „distrugere“ în loc de ceea ce numește „respectarea legii în mod tradițional“, cum ar fi strângerea de probe, tribunale și acuzații. Într-un document intitulat „Sesiune de ofensivă informatică: împingerea limitelor și acțiunea împotriva hacktivismului“, GCHQ discută despre luarea ca țintă a „hacktiviștilor“, ironic, prin atacuri de tip „negare a serviciului“, o tactică asociată în mod obișnuit cu hackerii:

De ce să se realizeze o astfel de operațiune

- Distrugere versus întărire a legii în mod tradițional
- SIGINT descoperă țintele
- Tehnicile de distrugere pot economisi timp și bani

TOP SECRET//COMINT//REL AUS/CAN/NZ/UK/US

Acțiune împotriva hacktivismului

- Op WEALTH – vara 2011
  - Sprijin cu informații pentru întărirea legii – identificarea țintelor principale
  - Negare a serviciului pe dispozitivele cheie de comunicare
  - Operațiuni de informare

TOP SECRET//COMINT//REL TO USA, AUS, CAN, GBR, NZL

Agenţia de supraveghere britanică folosește, de asemenea, o echipă de oameni de știinţă din domeniul social, inclusiv psihologi, pentru a elabora tehnici de „HUMINT online“ (human intelligence – activitate de spionaj privind fiinţa umană) și „distrugerea influenţei strategice“. Documentul „Arta înșelăciunii: Formare pentru o nouă generaţie de operaţiuni online sub acoperire“ este dedicată acestor tactici. Pregătit de HSOC (Celula de operaţiuni privind știinţele umane) a agenţiei, documentul pretinde că folosește sociologia, psihologia, antropologia, neuroștiinţa și biologia, printre alte domenii, pentru a maximiza abilităţile de inducere în eroare online ale GCHQ.

Un slide arată cum să folosești „Disimularea – Ascunde Realul“, propagând „Simularea – Arată Falsul“. Acesta examinează „construcţiile psihologice ale inducerii în eroare“ și „harta tehnologiilor“ folosite pentru a pune în aplicare înșelătorii, inclusiv pe Facebook, Twitter, LinkedIn și „pagini web“.

Subliniind că „oamenii iau decizii din motive emoţionale, nu raţionale“, în opinia GCHQ comportamentul online este determinat de „copiere“ („oamenii se copiază unii pe alţii în interacţiunea socială“), „adaptare“ și „mimetism“ („adoptarea unor trăsături sociale specifice de către comunicator de la alt participant“).

Documentul descrie apoi ceea ce numește „Operaţiunea de distrugere Playbook“, incluzând „operaţiuni de infiltrare“, „operaţiuni viclene“, „operaţiuni sub acoperire“ și „operațiuni de inducere în eroare“. Documentul promite o „lansare completă“ a programului de distrugere „la începutul lui 2013“, în timp ce „peste 150 de membri ai personalului sunt pe deplin antrenaţi“.

Purtând titlul „Tehnici magice & Experiment“, documentul se referă la „Legitimizarea violenţei“, „Construirea experienţei în mintea ţintei, care ar trebui acceptată fără ca ea să realizeze“ și „Optimizarea canalelor de inducere în eroare“.

Aceste tipuri de planuri guvernamentale de monitorizare și influenţare a comunicaţiilor pe internet și de diseminare

a unor informaţii false online au fost multă vreme o sursă de speculaţie. Profesorul de drept de la Harvard Cass Sunstein, un consilier apropiat al lui Obama, fost șef al Biroului pentru Informaţii și Afaceri Curente de la Casa Albă și numit în comisia de la Casa Albă pentru revizuirea activităţilor NSA, a scris un document controversat în 2008[34], în care propunea ca administraţia americană să folosească echipe de agenţi sub acoperire și avocaţi pseudo-„independenţi“ pentru a „se infiltra cognitiv“ în grupuri online, chat room, reţele de socializare și website, precum și în grupuri de activiști offline.

Toate dovezile subliniază târgul implicit oferit cetăţenilor: nu prezenta nici o provocare și nu ai de ce să te îngrijorezi. Vezi-ţi de treaba ta și sprijină sau cel puţin tolerează ceea ce facem și nu vei avea probleme. Cu alte cuvinte, trebuie să te abţii de la provocarea autorităţii care deţine puteri de supraveghere dacă vrei să fii considerat o persoană care nu provoacă nereguli. Acesta este un târg care invită la pasivitate, obedienţă și conformare. Cea mai sigură cale, modul de a te asigura că ești „lăsat în pace“, este să rămâi tăcut, neameninţător și supus.

Pentru mulţi, târgul este unul atractiv, convingând majoritatea că supravegherea este benignă sau chiar benefică. Sunt prea plictisitori pentru a atrage atenţia administraţiei, se gândesc ei. „Mă îndoiesc serios că NSA este interesată de mine“ este tipul de afirmaţie pe care o aud frecvent. „Dacă vor să urmărească viaţa mea plictisitoare, atunci sunt bine-veniţi“. Sau „NSA nu este interesată de bunica ta care vorbește despre reţetele ei sau de tatăl tău care își planifică partida de golf“.

Acestea sunt persoane care au devenit convinse că ele însele nu vor fi vizate personal – pentru că nu prezintă nici o ameninţare și sunt supuse – și fie neagă că acest lucru se întâmplă, fie nu le pasă, fie sunt dornice să sprijine pe loc acest lucru.

La scurt timp după apariţia subiectului NSA, moderatorul MSNBC Lawrence O'Donnell mi-a luat un interviu în timpul căruia a luat în derâdere noţiunea de NSA ca „un monstru

al supravegherii mare și înfricoșător“. Rezumând opinia sa, el a conchis:

> Sentimentul meu până acum este că... nu sunt speriat... faptul că administrația colectează [date] la un nivel atât de gigantic, masiv înseamnă că este chiar şi mai greu pentru administrație să mă găsească... şi nu are absolut nici un imbold să mă găsească. Astfel că, până în acest stadiu, mă simt complet neamenințat de acest lucru.[35]

Hendrik Hertzberg de la *New Yorker* a adoptat aceeași atitudine de desconsiderare a pericolelor supravegherii.[36] Acceptând că „nu există motive să fie îngrijorat în legătură cu raza de acţiune vastă a agenţiei, secretul excesiv și lipsa de transparenţă“ a acesteia, el a scris că „sunt și motive pentru a rămâne calm“, în special pentru că ameninţarea la adresa „libertăţilor civile, așa cum este ea, este abstractă, conjuncturală, nespecifică“. Iar editorialistul *Washington Post* Ruth Marcus, ridiculizând îngrijorările cu privire la puterile NSA, a anunţat – absurd – „metadatele mele aproape sigur nu au fost examinate“.[37]

Într-o măsură destul de mare, O'Donnell, Hertzberg și Marcus au dreptate. Este adevărat că administraţia SUA „nu are absolut nici un imbold“ să urmărească persoane ca ei, pentru care ameninţarea din partea statului supraveghetor este un pic mai mult decât „abstractă, conjuncturală, nespecifică“. Aceasta pentru că jurnaliștii care își dedică întreaga carieră venerării celui mai puternic oficial al ţării – președintele, care este comandantul-șef al NSA – și apărării partidului său politic rareori, sau chiar niciodată, riscă să îi îndepărteze pe cei de la putere.

Bineînţeles, susţinătorii loiali și ascultători ai președintelui și ai politicilor sale, buni cetăţeni care nu fac nimic să atragă atenţia negativă din partea celor puternici, nu au nici un motiv să se teamă de statul supraveghetor. Așa se întâmplă în orice societate: cei care nu prezintă nici o provocare sunt

rareori vizaţi de măsuri opresive, iar din perspectiva lor, pot să se convingă pe ei înșiși că opresiunea nu există cu adevărat. Dar adevărata măsură a libertăţii unei societăţi este dată de modul în care își tratează disidenţii și alte grupuri marginalizate, nu de felul în care își tratează supușii credincioși. Chiar și în cele mai rele tiranii din lume, susţinătorii ascultători sunt imuni la abuzurile puterii statale. În Egiptul lui Mubarak, cei care au ieșit pe străzi pentru a cere înlăturarea sa de la putere au fost arestaţi, torturaţi, împușcaţi; susţinătorii lui Mubarak și persoanele care au rămas tăcute acasă nu au fost supuse acestor practici. În Statele Unite, liderii NAACP, comuniștii și activiștii pentru drepturile civile și cei antirăzboi au fost vizaţi de supravegherea lui Hoover, nu cetăţenii care s-au comportat bine, care au rămas tăcuţi în faţa nedreptăţii sociale.

Nu ar trebui să fim supuși credincioși ai puterii pentru a ne simţi în siguranţă faţă de supravegherea statului. De asemenea, preţul imunităţii nu ar trebui să fie abţinerea de la opinii contrare și provocatoare. Nu ar trebui să ne dorim o societate în care mesajul transmis să fie că ești lăsat în pace doar dacă imiţi comportamentul servil și înţelepciunea convenţională a unui editorialist proguvernamental.

Dincolo de aceasta, sentimentul imunităţii resimţit de un grup anume aflat în prezent la putere este menit să fie iluzoriu. Acest lucru devine clar atunci când ne uităm cum afilierea partizană modelează sentimentul oamenilor cu privire la supravegherea de către stat. Ce reiese este că liderii iubiţi de ieri pot deveni rapid disidenţii de astăzi.

La momentul cotroversei din 2005 privind interceptarea fără mandat a NSA, liberalii și democraţii au considerat în mod covârșitor programul de supraveghere al agenţiei drept ameninţător. Parţial, bineînţeles, acest lucru se datorează partizanatului tipic al jurnaliștilor aserviţi: George W. Bush era președinte, iar democraţii au văzut o oportunitate de a da o lovitură politică lui și partidului său. Dar o parte semnificativă din teama lor era reală: pentru că l-au considerat pe Bush rău

intenţionat și periculos, ei au perceput supravegherea de către statul aflat sub controlul lui ameninţătoare și s-au simţit în pericol ca oponenţi politici. În mod echivalent, republicanii au avut o opinie mai blândă și de susţinere pentru acţiunile NSA. În decembrie 2013, în schimb, democraţii și progresiștii s-au convertit în apărători ai NSA.

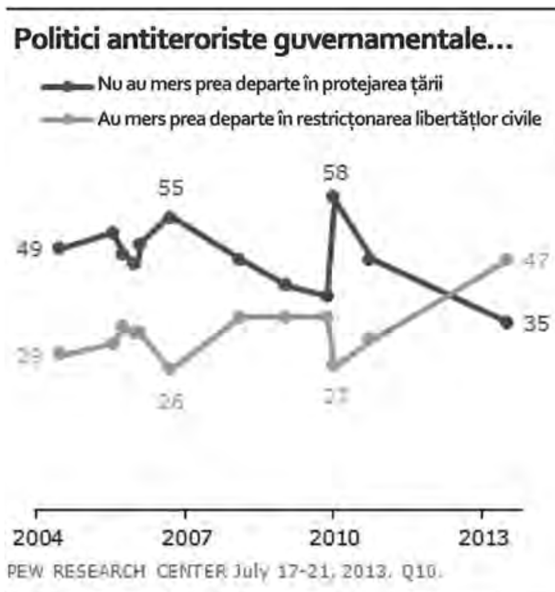
Sondaje de opinie ample reflectă această schimbare. La sfârșitul lui iulie 2013, Pew Research Center a realizat un sondaj care arată că majoritatea americanilor nu cred în pledoariile oferite în favoarea NSA. În particular, „majoritatea americanilor – 56% – susţin că tribunalele federale nu reușesc să furnizeze limite adecvate pentru datele telefonice și de internet pe care administraţia le colectează în cadrul eforturilor sale antiterorism“.[38] Și „o proporţie chiar și mai mare (70%) crede că administraţia folosește aceste date în alte scopuri decât investigarea terorismului“. Mai mult, „63% cred că administraţia strânge informaţii despre conţinutul comunicaţiilor“.

Cel mai remarcabil este că americanii consideră acum pericolul supravegherii o sursă de îngrijorare mai mare decât pericolul terorismului:

> În total, 47% afirmă că îngrijorarea cea mai mare cu privire la politicile guvernamentale antiterorism este că acestea au mers prea departe în restricționarea libertăților civile ale persoanelor, în timp ce 35% susțin că sunt mai îngrijorați că politicile nu au mers suficient de departe pentru a proteja țara. Este pentru prima dată când, într-un sondaj al Pew Research, mai multe persoane şi-au exprimat îngrijorarea în privința libertăților civile decât a protecției față de terorism de la introducerea acestei întrebări, în 2004.

Aceste rezultate au fost o veste bună pentru oricine era alarmat de folosirea excesivă a puterilor guvernamentale și de exagerarea cronică a ameninţării terorismului. Dar au subliniat și o inversiune grăitoare: republicanii, care au fost apărători ai NSA în timpul lui Bush, au fost înlocuiţi de democraţi,

odată ce sistemul de supraveghere a intrat sub controlul președintelui Obama, unul de-ai lor. „La nivel național, există mai mult sprijin pentru programul guvernamental de colectare a datelor în rândul democraților (57% îl aprobă) decât al republicanilor (44%)".



Un sondaj similar de la *Washington Post*[39] dezvăluie cum conservatorii au fost mult mai îngrijorați de programul de spionaj al NSA decât liberalii. Întrebați „Cât de îngrijorat sunteți, dacă sunteți, în legătură cu colectarea și folosirea datelor dumneavoastră personale de către Agenția pentru Securitate Națională?", 48% dintre conservatori s-au declarat „foarte îngrijorați" comparativ cu doar 26% dintre liberali. Așa cum menționa profesorul de drept Orin Kerr, aceasta a reprezentat o schimbare fundamentală: „Este o inversare interesantă față de 2006, când președinte era un republican în loc de un democrat. Atunci, un sondaj Pew arăta că 75% dintre republicani

aprobă supravegherea NSA, dar numai 37% dintre democraţi o aprobă“[40].

Un grafic al Pew arată clar această schimbare:

Schimbări în viziunea partidelor cu privire la programele de supraveghere ale NSA

Păreri cu privire la programele de supraveghere ale NSA

	Ianuarie 2006		*Ianuarie 2013*	
	Acceptabil	**Inacceptabil**	**Acceptabil**	**Inacceptabil**
	%	%	%	%
Total	51	47	56	41
Republicani	75	23	52	47
Democraţi	37	61	64	34
Independenţi	44	55	53	44

PEW RESEARCH CENTER June 6-9, 2013. Figures read across. Don't know/Refused responses not shown.

Argumentele pentru și împotriva supravegherii pivotează cinic în funcţie de ce partid este la putere. Colectarea de metadate în masă de către NSA a fost denunţată vehement de un senator[41] în *Face the Nation* în 2006 astfel:

> Nu trebuie să îți ascult apelurile telefonice ca să ştiu ce faci. Dacă ştiu fiecare telefon pe care îl dai, pot să stabilesc fiecare persoană cu care ai vorbit. Pot obține un tipar al vieții tale care este foarte, foarte intruziv... Iar întrebarea reală este: ce fac ei cu aceste informații pe care le colectează şi care nu au nimic de-a face cu al-Qaeda?... Şi trebuie să avem încredere în preşedintele şi vicepreşedintele Statelor Unite că vor face ce trebuie? Nu contați pe mine pentru aceasta.

Senatorul care ataca atât de dur colectarea de metadate era Joe Biden, care ulterior, ca vicepreședinte, a devenit parte a administraţiei democrate ce a avansat exact același tip de argumente pe care odinioară le lua în derâdere.

Ideea relevantă aici nu este că mulţi susţinători loiali sunt ipocriţi fără principii și fără nici o altă convingere reală decât căutarea puterii, deși acest lucru este cu siguranţă adevărat. Mai important este ce dezvăluie aceste declaraţii despre natura modului în care cineva vede supravegherea de către stat. Cu atât de multe nedreptăţi, oamenii sunt dornici să discrediteze teama de depășire a atribuţiilor guvernamentale atunci când cred că oamenii care se întâmplă să fie la control sunt binevoitori și de încredere. Ei consideră supravegherea periculoasă sau capabilă să provoace îngrijorare doar atunci când percep că ei înșiși sunt ameninţaţi de ea.

Extinderile radicale ale puterii sunt deseori introduse în acest fel, convingând oamenii că acestea afectează doar un grup specific, discret. Guvernele au convins multă vreme populaţia să ignore modul opresiv de conducere îndreptând cetăţenii să creadă, în mod greșit, că doar unele persoane marginalizate sunt vizate și că toţi ceilalţi pot accepta sau chiar susţine această opresiune fără teama că ea le va fi aplicată lor. Lăsând deoparte neajunsurile morale evidente ale acestei poziţii – nu respingem rasismul pentru că este îndreptat împotriva unei minorităţi sau nu ignorăm foametea din unele zone pentru că noi ne bucurăm de suficientă mâncare –, aceasta este aproape întotdeauna greșită din punct de vedere pragmatic.

Indiferenţa sau sprijinul celor care cred că ei înșiși sunt scutiţi permite invariabil ca abuzul de putere să se extindă dincolo de aplicarea sa iniţială, până când abuzul devine imposibil de controlat – așa cum se va întâmpla în mod inevitabil. Sunt prea multe exemple, dar poate cel mai recent și mai convingător este exploatarea Patriot Act. Congresul a aprobat aproape în unanimitate creșterea puterilor în domeniul supravegherii și detenţiei după 11 septembrie, convins de argumentul că în acest fel vor fi detectate și prevenite viitoarele atacuri.

Presupunerea implicită era că aceste puteri vor fi folosite în principal împotriva musulmanilor care au legături cu terorismul – o extindere clasică a puterii limitate la un grup

anume implicat într-un tip specific de acţiune –, acesta fiind unul dintre motivele pentru care măsura a primit o susţinere covârșitoare. Dar ce s-a întâmplat a fost diferit: Patriot Act a fost o lege aplicată dincolo de scopul său aparent. De fapt, de la intrarea sa în vigoare, legea a fost folosită în mod covârșitor în cazuri care nu aveau nimic de-a face cu terorismul sau securitatea naţională. *New York Magazine* a dezvăluit că, din 2006 și până în 2009, prevederea „furișează-te și aruncă o privire" (menită să execute un mandat de căutare fără informarea imediată a ţintei) a fost folosită în 1 618 cazuri legate de droguri, în 122 de cazuri referitoare la fraudă și doar în 15 au implicat terorismul[42].

Dar odată ce cetăţenii acceptă noua putere, crezând că aceasta nu îi afectează, ea devine instituţionalizată și legitimată, iar obiecţia devine imposibilă. Într-adevăr, lecţia esenţială oferită de Frank Church în 1975 a fost amploarea pericolului reprezentat de supravegherea în masă. Într-un interviu acordat în cadrul emisiunii *Meet the Press*, el afirma:

> Această capacitate poate fi întoarsă în orice moment împotriva americanilor şi nici un american nu va mai avea intimitate, atât de mare este capacitatea de a monitoriza orice – conversații telefonice, telegrame, nu contează. Nu va mai exista nici un loc în care să te ascunzi. Dacă această administrație devine vreodată un tiran... capacitatea tehnologică pe care comunitatea de informații i-a dat-o administrației i-ar permite acesteia să impună o tiranie totală şi nu va mai exista nici o modalitate de a riposta, pentru că și cel mai atent efort de a te reuni în rezistență... ajunge să fie cunoscut de administrație. Atât de mare este capacitatea acestei tehnologii.[43]

Scriind în *New York Times* în 2005, James Bamford a remarcat că ameninţarea din partea supravegherii statului este mult mai alarmantă astăzi decât era în 1970: „Cu oamenii care își exprimă cele mai intime gânduri în mesaje electronice, dezvăluindu-și datele medicale și financiare pe internet și vorbind

constant la telefon, agenţia are practic capacitatea de a intra în mintea unei persoane“[44].

Îngrijorarea lui Church, că orice capacitate de supraveghere „se poate întoarce împotriva cetăţenilor americani“, este exact ceea ce a făcut NSA după 11 septembrie. În pofida faptului că operează în conformitate cu Legea privind supravegherea activităţii de informaţii străine și în ciuda interzicerii spionajului intern, prevedere înscrisă în misiunea agenţiei de la început, multe dintre activităţile de supraveghere se concentrează acum pe cetăţeni americani aflaţi pe teritoriul SUA.

Chiar și fără abuzuri și chiar dacă cineva nu este urmărit personal, un stat supraveghetor care colectează tot dăunează societăţii și libertăţii politice în general. În Statele Unite și în alte ţări au fost realizate progrese doar prin posibilitatea de a contesta puterea și dogmele și de a crea noi căi de gândire și existenţă. Toţi, inclusiv cei care nu sunt implicaţi în militantism contestatar sau activism politic, suferă atunci când libertatea este înăbușită de teama de a fi urmărit. Hendrik Hertzberg, care a minimalizat îngrijorările cu privire la programele NSA[45], recunoaște totuși că „răul a fost făcut. Răul este civic. Răul este colectiv. Răul este făcut la adresa arhitecturii încrederii și responsabilităţii care susţin o societate deschisă și democratică“.

Susţinătorii supravegherii oferă în esenţă un singur argument în favoarea supravegherii în masă: aceasta este desfășurată doar pentru a opri terorismul și a menţine siguranţa oamenilor. Într-adevăr, invocarea unei ameninţări externe este o tactică istorică aleasă pentru a menţine populaţia docilă în faţa puterii guvernamentale. Administraţia americană a invocat pericolul terorismului mai mult de un deceniu pentru a justifica mulţimea de acte radicale, de la extrădări și torturi la asasinări și invadarea Irakului. Mereu, de la atacurile din 11 septembrie, oficialii americani au reprodus din reflex cuvântul „terorism“. Este tot mai mult un slogan și o tactică

decât un argument concret sau o justificare convingătoare a acţiunii. Iar în cazul supravegherii, dovezi covârșitoare arată cât de dubioasă este o justificare.

Mai întâi, mare parte din colectarea de date desfășurată de NSA nu are nimic de-a face cu terorismul sau cu securitatea naţională. Interceptarea comunicaţiilor gigantului petrolier brazilian Petrobras sau spionarea sesiunilor de negocieri la un summit economic sau urmărirea unor lideri aleși democratic în state aliate sau colectarea tututor datelor comunicaţiilor americanilor nu are legătură cu terorismul. Având în vedere supravegherea pe care o desfășoară în prezent NSA, oprirea terorismului este clar un pretext.

Mai mult, argumentul că supravegherea în masă a prevenit comploturi teroriste – o afirmaţie făcută de președintele Obama și de o serie de figuri din cadrul securităţii naţionale – s-a dovedit a fi fals. Așa cum menţiona *Washington Post* în decembrie 2013, într-un articol intitulat „Apărarea de către oficiali a programului telefonic al NSA poate fi destructurată“, un judecător federal a declarat programul de colectare a metadatelor telefonice „aproape sigur“ neconstituţional, afirmând că Departamentul de Justiţie a eșuat în a „cita un singur caz în care analizarea metadatelor colectate în masă de către NSA a oprit de fapt un atac terorist iminent“[46].

În aceeași lună, un comitet consultativ selectat de Obama (format, între alţii, dintr-un fost director adjunct al CIA și un fost consilier la Casa Albă, și desemnat să analizeze programul NSA prin acces la informaţii secretizate) a conchis că programul de metadate „nu avea ca scop în mod esenţial prevenirea unor atacuri și ar fi putut fi obţinut ușor în mod corespunzător folosind ordine [judecătorești] convenţionale“.[47]

Citând *The Post* din nou: „În mărturia depusă în faţa Congresului, [Keith] Alexander a creditat programul cu contribuţia la detectarea a zeci de comploturi atât în Statele Unite, cât și peste hotare“, dar raportul consiliului consultativ „retează adânc din credibilitatea acestor afirmaţii“.[48]

În plus, așa cum au afirmat direct în *New York Times* senatorii Ron Wyden, Mark Udall și Martin Heinrich – toţi membri ai Comisiei pentru Serviciile de informaţii –, colectarea în masă a datelor telefonice nu a sporit protecţia americanilor în faţa ameninţării terorismului.

> Utilitatea programului de colectare în masă a fost mult exagerată. Nu am văzut încă nici o dovadă care să ateste valoarea unică şi reală a acestuia pentru protejarea securității naționale. În pofida cererilor noastre repetate, NSA nu a oferit dovezi de nici un fel atunci când agenția a folosit acest program pentru a urmări date telefonice care nu ar fi putut fi obținute folosind un ordin judecătoresc obişnuit sau o autorizație de urgență.[49]

Un studiu al Fundaţiei New America[50], de centru, care testează veridicitatea justificărilor oficiale pentru colectarea în masă a metadatelor a conchis că programul „nu are un impact vizibil asupra prevenirii actelor de terorism“. În schimb, așa cum menţiona *Washington Post*, în majoritatea cazurilor în care au fost dejucate comploturi[51], studiul a descoperit că „metodele de investigare tradiţionale și care respectă legea au oferit indiciul sau dovada iniţierii cazului“.

Palmaresul este într-adevăr slab. Sistemul colectează tot nu a făcut nimic pentru a depista, ca să nu mai vorbim pentru a dejuca, atentatul din 2012 de la Maratonul din Boston. Nu a făcut nimic pentru a depista încercarea de atac din ziua de Crăciun de la bordul unui avion în Detroit sau planul de aruncare în aer a Times Square sau complotul privind sistemul de transport subteran din New York – toate au fost oprite de trecători alarmaţi sau de forțe poliţienești tradiţionale. Cu siguranţă nu a făcut nimic pentru a opri șirul de incidente armate de la Aurora la Newtown. Atacurile internaţionale majore de la cel din Londra până la cele din Mumbai sau Madrid s-au desfășurat fără a fi depistate, în pofida implicării a zeci de persoane.

Și în pofida afirmaţiilor bombastice ale NSA, supravegherea în masă nu a oferit serviciilor de informaţii instrumente mai bune pentru a preveni atacul din 11 septembrie. Keith Alexander, vorbind în faţa unei comisii a Senatului, a declarat: „Mai bine să fiu astăzi aici pentru a dezbate“ programul „decât să încerc să explic cum am eșuat în a preveni un alt 11 septembrie“[52]. (Același argument, potrivit înregistrărilor, a apărut în instrucţiunile pe care NSA le-a dat angajaţilor săi pentru a evita întrebările.)

Implicaţia este extrem de alarmistă și dezamăgitoare. Așa cum a arătat analistul CNN în domeniul securităţii Peter Bergen[53], CIA a avut rapoarte multiple despre un complot al-Qaeda și „câteva informaţii despre doi dintre atacatori și despre prezenţa lor în Statelor Unite“ pe care „agenţia nu le-a împărtășit altor agenţii guvernamentale până când a fost prea târziu pentru a se mai face ceva“.

Lawrence Wright, expert în al-Qaeda la *New Yorker*, a demitizat afirmaţia NSA că prin colectarea de metadate s-ar fi oprit atacurile din 11 septembrie, explicând că CIA „a ascuns informaţii cruciale de FBI, care are autoritatea ultimă de a investiga terorismul pe teritoriul SUA și atacurile asupra americanilor din străinătate“[54]. FBI ar fi putut opri 11 septembrie, a argumentat el.

> Avea mandat pentru a pune sub supraveghere orice persoană cu legături cu al-Qaeda din America. I-ar fi putut urmări, le-ar fi putut intercepta telefoanele, clona computerele, citi e-mailurile şi datele medicale, bancare şi de credit. Avea dreptul să ceară înregistrări de la companiile de telefonie pentru orice apel pe care îl făcuseră. Nu era nevoie de un program de colectare de metadate. Era nevoie de cooperare cu alte agenții federale, dar, din motive meschine şi obscure, aceste agenții au ales să ascundă de investigatori indicii vitale, care cel mai probabil ar fi prevenit atacurile.

Administraţia se afla în posesia informaţiilor necesare, dar a eșuat în a înţelege sau a acţiona. Soluţia folosită de atunci – de a colecta totul, în masă – nu a făcut nimic pentru a rezolva acest eșec.

De nenumărate ori, din unghiuri multiple, invocarea ameninţării terorismului pentru a justifica supravegherea a fost expusă ca o pavăză.

De fapt, supravegherea în masă are tocmai efectul opus: face detectarea și oprirea terorismului mai dificile. Congresmenul democrat Rush Holt, fizician și unul dintre puţinii oameni de știinţă din Congres, a subliniat că o colectare generală a comunicaţiilor tuturor doar ascunde comploturile reale despre care discută teroriștii reali.[55] Supravegherea direcţionată mai degrabă decât cea fără discriminare, ar putea aduce informaţii mai specifice și mai folositoare. Abordarea actuală inundă agenţiile de informaţii cu atât de multe date, încât acestea nu le pot sorta eficient.

Dincolo de faptul că furnizează prea multe informaţii, schemele de supraveghere ale NSA au sfârșit prin a crește vulnerabilitatea ţării: eforturile agenţiei de a sparge metodele de criptare care protejau tranzacţiile obișnuite pe internet – cum ar fi cele bancare, datele medicale și comerciale – au lăsat aceste sisteme deschise la infiltrarea hackerilor și a altor entităţi ostile.

Expertul în securitate Bruce Schneier, scriind în *Atlantic* în ianuarie 2014, sublinia:

> Nu numai că supravegherea generalizată este ineficientă, dar este şi extraordinar de costisitoare. Ea sparge sistemele noastre tehnice, astfel că fiecare protocol al internetului devine unul pe care nu te poţi bizui... Nu este doar un abuz intern în legătură cu care trebuie să ne îngrijorăm; este vorba şi despre restul lumii. Cu cât alegem să ascultăm comunicațiile pe internet şi prin alte tehnologii, cu atât mai puțin suntem în siguranță față de interceptarea de către alții. Alegerea noastră nu este între o lume digitală în care NSA poate să spioneze şi una în care NSA

> este împiedicată să facă acest lucru; ci este între o lume digitală vulnerabilă la toți atacatorii şi una care este sigură pentru toți utilizatorii.[56]

Poate cel mai remarcabil lucru în legătură cu exploatarea nelimitată a ameninţării terorismului este că aceasta este mult exagerată. Riscul ca un american să moară într-un atac terorist este infinit mai mic decât acela de a fi lovit de fulger. John Mueller, profesor la Universitatea de Stat din Ohio, care a scris pe larg despre balanţa între ameninţare și cheltuieli în combaterea terorismului, a explicat în 2012: „Numărul persoanelor din întreaga lume care sunt ucise de teroriști musulmani adepţi ai al-Qaeda este poate de câteva sute în afara zonelor de război. Este practic același număr de persoane care mor înecate în cadă în fiecare an“[57].

Au murit „indubitabil“ mai mulţi americani „peste hotare în accidente rutiere sau de boli intestinale“, anunţă agenţia de știri McClatchy, „decât din cauza terorismului“.[58]

Ideea că trebuie să destructurăm protecţiile centrale ale sistemului nostru politic pentru a construi un stat al supravegherii generalizate în numele acestui risc este apogeul iraţionalului. Cu toate acestea, exagerarea ameninţării este repetată mereu. Cu puţin timp înainte de Jocurile Olimpice de la Londra din 2012 a apărut controversa cu privire la lipsa de securitate. Compania contractată pentru a garanta securitatea nu a reușit să angajeze numărul de agenți cerut de contract, iar voci stridente din întreaga lume au insistat că jocurile sunt, prin urmare, vulnerabile la un atac terorist.

După ce Jocurile Olimpice s-au desfășurat fără tulburări, Stephen Walt a subliniat în *Foreign Policy*[59] că protestele au fost determinate, ca de obicei, de exagerarea severă a ameninţării. El a citat un eseu al lui John Mueller și Mark G. Stewart în *International Security* pentru care autorii au analizat 50 de cazuri de presupuse „comploturi teroriste islamice“ împotriva Statelor Unite, doar pentru a conchide că „de fapt, toţi autorii

au fost «incompetenţi, ineficienţi, lipsiţi de inteligenţă, stupizi, ignoranţi, neorganizaţi, induși în eroare, confuzi, amatori, dopaţi, nerealiști, imbecili, iraţionali și proști»“. Mueller și Stewart au citat din Glenn Carle, fost adjunct al ofiţerului pentru informaţii interne pentru ameninţări transnaţionale, care a spus: „Trebuie să vedem jihadiștii ca pe niște oponenţi mici, letali, dezorganizaţi și jalnici, ceea ce și sunt“, și a menţionat că „înzestrările al-Qaeda sunt mult inferioare dorinţelor sale“.

Problema, totuși, este că sunt mult prea multe facţiuni de putere cu interesul legitim de a menţine teama faţă de terorism: guvernul, care încearcă să își justifice acţiunile; industriile de supraveghere și armament, care beneficiază de fonduri publice; și permanentele facţiuni de putere de la Washington, angajate în stabilirea priorităţilor lor fără o provocare reală. Stephen Walt a afirmat:

> Conform estimărilor lui Mueller şi Stewart, cheltuielile pentru securitatea internă (fără a pune la socoteală războaiele din Irak sau Afghanistan) au crescut cu peste un trilion de dolari din 11 septembrie, chiar dacă riscul anual de a muri într-un atac terorist pe teritoriul SUA este de circa 1 la 3,5 milioane. Folosind presupunerile conservatoare şi metodologia convențională de evaluare a riscului, ei estimează că pentru justificarea acestor cheltuieli „ar trebui să descurajeze, să prevină, să dejoace sau să protejeze împotriva a 333 de atacuri la scară foarte mare care altfel s-ar realiza cu succes în fiecare an“. În plus, ei sunt îngrijorați că acest simț exagerat al pericolului a fost „internalizat“: chiar şi atunci când politicienii şi „experții în terorism“ nu amplifică pericolul, publicul încă vede amenințarea ca fiind mare şi iminentă.

În timp ce frica de terorism a fost manipulată, pericolele dovedite ale permisiunii acordate statului de a opera un sistem masiv și secret de supraveghere au fost grav subestimate.

Chiar dacă ameninţarea terorismului ar fi la nivelul pretins de administraţie, aceasta nu ar justifica programele de supraveghere ale NSA. Alte valori decât siguranţa fizică sunt la fel, dacă nu chiar mai importante. Această recunoaștere a fost înrădăcinată în cultura politică americană de la crearea naţiunii și nu este mai puţin importantă pentru alte ţări.

Naţiuni și indivizi fac în mod constant alegeri care plasează intimitatea și, implicit, libertatea înaintea altor obiective, cum ar fi siguranţa fizică. Într-adevăr, scopul celui de-al Patrulea Amendament al Constituţiei SUA este să interzică unele acţiuni ale poliţiei, chiar dacă acestea ar putea reduce criminalitatea. Dacă poliţia ar putea intra în orice casă fără mandat, criminalii, violatorii și răpitorii ar putea fi prinși mai ușor. Dacă statului i s-ar permite să amplaseze monitoare în casele noastre, criminalitatea ar scădea probabil semnificativ (acest lucru este cu siguranţă adevărat în cazul spargerilor de locuinţe, deși majoritatea oamenilor ar fi oripilaţi de această perspectivă). Dacă FBI i s-ar permite să ne asculte conversaţiile, să ne confiște comunicaţiile, o arie largă de infracţiuni ar fi în mod clar prevenite și rezolvate.

Dar Constituţia a fost scrisă pentru a preveni astfel de invazii fără temei ale statului. Neacceptând intruziunea statului, permitem în mod conștient probabilitatea unei infracționalități mai mari. Cu toate acestea, ne asumăm decizia păstrării intimității, expunându-ne la un grad mai mare de pericol pentru că urmărirea unei siguranţe fizice absolute nu a fost niciodată singura noastră prioritate la nivel de societate.

Dincolo chiar de integritatea noastră fizică, o valoare centrală ţine statul departe de viaţa privată – „persoanele, locuinţele, documentele și bunurile“ noastre așa cum stabilește al Patrulea Amendament. Facem acest lucru tocmai pentru că acest tărâm este creuzetul atâtor atribute, asociat în mod tipic cu calitatea vieţii – creativitate, explorare, intimitate.

Renunţarea la intimitate în căutarea unei siguranţe absolute este dăunătoare pentru sănătatea psihică și viaţa unui

individ, așa cum este și pentru o cultură politică sănătoasă. Pentru individ, siguranţa înseamnă în primul rând o viaţă de paralizie și teamă, să nu urce niciodată la bordul unei mașini sau al unui avion, să nu se implice niciodată într-o activitate care presupune riscuri, să nu acorde mai multă greutate calităţii vieţii decât cantităţii, să plătească orice preţ pentru a evita pericolul.

Alarmismul este o tactică favorită a autorităţilor tocmai pentru că teama justifică atât de convingător extinderea puterii și reduce drepturile. De la începutul războiului împotriva terorismului, americanilor li s-a spus frecvent că trebuie să renunţe la esenţa drepturilor lor politice dacă vor să aibă vreo speranţă de a evita o catastrofă. De către președintele Comisiei pentru Serviciile de informaţii din Senat, Pat Roberts, de exemplu: „Sunt un susţinător puternic al Primului Amendament, al celui de-al Patrulea Amendament și al libertăţilor civile. Dar nu ai libertăţi civile dacă ești mort".[60] Iar senatorul republican John Cornyn, care a candidat pentru a fi reales în Texas cu o înregistrare video cu el pozând în bărbat dur cu pălărie de cowboy, a închinat o odă lașă beneficiilor obţinute prin renunţarea la drepturi[61]: „Nici una dintre libertăţile tale civile nu contează prea mult după ce mori".

Rush Limbaugh, gazda unei emisiuni de radio, li s-a alăturat[62], arătând o ignoranţă istorică atunci când și-a întrebat publicul: „Când a fost ultima dată când aţi auzit un președinte că declară război în baza faptului că trebuie să mergem să ne protejăm libertăţile civile? Eu nu știu nici unul... Libertăţile noastre civile nu au nici o valoare dacă suntem morţi! Dacă ești mort și acoperit cu margarete, dacă ești acoperit cu pământ în interiorul unei lăzi, știi cât valorează libertăţile tale civile? Zilch, zero, nada."

O populaţie, o ţară care venerează siguranţa fizică înaintea tuturor celorlalte valori va renunţa în cele din urmă la libertatea sa și va aproba orice putere confiscată de autoritate în schimbul unei promisiuni, indiferent cât de iluzorie ar fi

aceasta, de siguranţă totală. Totuși, siguranţa absolută este himerică în sine, urmărită, dar niciodată obţinută. Urmărirea ei îi afectează pe cei implicaţi în cursă la fel ca pe orice naţiune care ajunge să fie definită de ea.

Pericolul reprezentat de statul care desfășoară un sistem secret de supraveghere masivă este mult mai ameninţător acum decât în orice alt moment din istorie. În timp ce guvernul, prin supraveghere, știe din ce în ce mai multe despre ce fac cetăţenii săi, cetăţenii știu din ce în ce mai puţine despre ce face guvernul lor, protejat așa cum este de un zid al secretului.

Este greu să evaluezi cât de radical răstoarnă această situaţie dinamica definitorie a unei societăţi sănătoase sau cât de fundamental schimbă echilibrul puterilor în favoarea statului. Panopticonul lui Bentham, menit să învestească autorităţile cu o putere de necombătut, s-a bazat tocmai pe această inversare: „Esenţa acesteia", scrie el, rezidă în „locul central al situaţiei inspectorului"[63] combinat cu „cele mai eficiente născociri pentru a vedea fără să fii văzut".

Într-o democraţie sănătoasă este adevărat tocmai opusul. Democraţia cere responsabilitate și consimţământ din partea celor guvernaţi, care sunt posibile dacă cetăţenii știu ce se face în numele lor. Se pleacă de la presupunerea, cu rare excepţii, că ei vor ști tot ce fac oficialii lor politici, care de aceea se numesc funcţionari publici, care lucrează în sectorul public, în serviciul publicului, pentru agenţii publice. În schimb, se presupune că guvernul, cu rare excepţii, nu va ști tot ce fac cetăţenii care se supun legii. De aceea suntem numiţi persoane private, acţionând în conformitate cu capacitatea noastră privată. Transparenţa este pentru cei care desfășoară activităţi publice și exercită puteri publice. Intimitatea este pentru toţi ceilalţi.

Capitolul 5

A patra putere

Una dintre principalele instituţii dedicate în mod evident monitorizării și verificării abuzului puterii statului este mass-media politică. Teoria celei de-a „patra puteri“ ar trebui să asigure transparenţă guvernamentală și să ofere un control asupra depășirii atribuţiilor, iar supravegherea secretă a întregii populaţii este cu siguranţă printre cele mai radicale exemple. Dar acest control este eficient doar dacă jurnaliștii acţionează critic faţă de cei care deţin puterea politică. În schimb, presa americană a abdicat frecvent de la acest rol, fiind servilă faţă de interesele administraţiei, chiar amplificând mai degrabă decât să examineze mesajele sale și făcând treaba murdară a acesteia.

În acest context, am știut că ostilitatea presei faţă de relatările mele despre dezvăluirile lui Snowden este inevitabilă. La 6 iunie, la o zi după apariţia primului articol despre NSA în *Guardian*, *New York Times* a introdus posibilitatea unei anchete penale.[1] „După ce a scris intens, chiar obsesiv, ani la rând despre supravegherea guvernamentală și urmărirea judiciară a jurnaliștilor, Glenn Greenwald s-a plasat brusc direct la intersecţia acestor două subiecte și poate în vizorul procurorilor federali“, proclama ziarul într-un profil pe care mi l-a realizat. Relatarea mea despre NSA, adăuga acesta, „este de așteptat să atragă o anchetă din partea Departamentului de Justiţie, care a urmărit în mod agresiv autorii scurgerilor de informaţii“. Profilul îl cita pe neoconservatorul Gabriel Schoenfeld de la Institutul Hudson, care a susţinut multă vreme urmărirea judiciară a jurnaliștilor pentru publicarea de informaţii secrete,

numindu-mă un „apologet foarte profesional al oricărui tip de antiamericanism, indiferent cât de extrem este acesta“.

Cea mai revelatoare dovadă a intenţiilor *Times* a venit din partea jurnalistului Andrew Sullivan, care a fost citat în același profil spunând: „Odată ce intri într-o dezbatere cu [Greenwald], poate fi dificil să ai ultimul cuvânt“ și „eu cred că nu are idee despre ce înseamnă de fapt să guvernezi o ţară sau să duci un război“. Deranjat de folosirea comentariilor sale scoase din context, Andrew mi-a trimis schimbul de replici integral pe care l-a avut cu reporterul *Times* Leslie Kaufman, care includea laude la adresa activităţii mele pe care ziarul a ales în mod evident să le omită. Și mai grăitoare însă erau întrebările pe care Kaufman i le trimisese:

> „În mod evident, el are opinii puternice, dar cum este ca jurnalist? Este de încredere? Onest? Te citează corect? Descrie corect pozițiile tale? Sau este mai mult avocat decât jurnalist?“
>
> „El spune că îi eşti prieten, aşa este? Am sentimentul că este un singuratic şi are tipul de opinii intransigente care te împiedică să îți păstrezi prietenii, dar este posibil să mă înşel.“

A doua întrebare – că sunt „un singuratic“ care are probleme în a-și păstra prietenii – era, într-o anumită măsură, chiar mai semnificativă decât prima. Discreditarea mesagerului ca inadaptabil pentru a discredita mesajul este o tactică veche atunci când vine vorba despre avertizorii de integritate și deseori funcţionează.

Efortul de a mă discredita a fost deplin atunci când am primit un e-mail de la un reporter al *New York Daily News*. El a spus că investighează diverse aspecte ale trecutului meu, inclusiv datoriile, responsabilitatea privind taxele și parteneriatul pe care îl are o corporaţie privată la care am deținut acţiuni în urmă cu opt ani cu o companie de distribuţie de filme pentru adulţi. Pentru că *Daily News* este un tabloid care deseori face comerţ cu chestiuni personale în mod imoral, am decis să nu

răspund: nu există nici un motiv pentru a atrage mai multă atenţie asupra problemelor pe care le-a ridicat.

Dar în aceeași zi am primit un e-mail de la un reporter al *Times*, Michael Schmidt, interesat de asemenea să scrie despre trecutul meu cu privire la datoriile privind taxele. Cum au aflat simultan cele două ziare despre detalii atât de obscure era un mister, dar *Times* a decis în mod evident că datoria mea anterioară merita o știre – chiar dacă a refuzat să spună de ce.

Aceste subiecte erau triviale și aveau intenţia de a defăima. *Times* a sfârșit prin a nu mai publica povestea, spre deosebire de *Daily News*, care a inclus chiar și detalii despre un conflict pe care l-am avut în clădirea de apartamente în care locuiam în urmă cu zece ani în legătură cu afirmaţia că am un câine care depășește limita de greutate admisă de regulile administrative ale complexului.

În timp ce campania de defăimare era previzibilă, efortul de a nega statutul meu de jurnalist nu era, și a avut ramificaţii destul de serioase. Încă o dată, această campanie a fost iniţiată de *New York Times*, tot în profilul din 6 iunie. În titlul articolului, ziarul a mers până acolo încât mi-a atribuit un titlu nejurnalistic: „Blogger, cu preocupare pentru supraveghere, este în centrul unei dezbateri“. Pe cât de prost era titlul, originalul de pe online era și mai mult decât atât: „Activist antisupraveghere este în centrul unei noi scurgeri de informaţii“.

Margaret Sullivan, redactor responsabil cu respectarea normelor de etică, a criticat titlul, afirmând că îl consideră „dispreţuitor“. Ea a spus: „Nu este nimic greșit în a fi blogger, bineînţeles – și eu sunt. Dar când presa consacrată folosește termenul, este ca și cum ai spune «nu ești chiar unul de-ai noștri»“.[2]

Articolul a încercat în mod repetat să mă prezinte drept altceva decât un „jurnalist“ sau „reporter“. Am fost, afirma acesta, un „avocat și multă vreme un blogger“ (nu am practicat dreptul de șase ani și am lucrat ani la rând ca editorialist la organizaţii de presă importante, pe lângă publicarea a patru

cărţi). În ceea ce privește perioada în care am lucrat „ca jurnalist", susţinea ziarul, experienţa mea era „neobișnuită", nu din cauza „opiniilor mele clare", ci pentru că „rareori am dat socoteală unui redactor".

Apoi presa în ansamblu a intrat într-o dezbatere dacă am fost de fapt „jurnalist" sau altceva. Alternativa oferită cel mai des era cea de „activist". Nimeni nu s-a deranjat să definească aceste cuvinte, bazându-se în schimb pe clișee prost definite, așa cum tinde să facă presa, mai ales atunci când scopul este discreditarea. După aceea, eticheta goală și anostă este aplicată în mod curent.

Această etichetare a avut o semnificaţie reală la câteva niveluri. În primul rând, contestarea statutului de „jurnalist" diminuează legitimitatea relatării. Mai mult, transformarea mea în „activist" ar putea avea consecinţe legale – adică penale. Există protecţii atât formale, cât și nescrise oferite jurnaliștilor care nu sunt valabile pentru altcineva. În timp ce, în general, se consideră că este legitim ca un jurnalist să publice secrete guvernamentale, de exemplu, acest lucru nu este valabil pentru cineva care acţionează în altă calitate.

Intenţionat sau nu, promovarea ideii că nu sunt jurnalist – în pofida faptului că am scris pentru unul dintre cele mai mari ziare din lumea occidentală – a ușurat posibilitatea ca administraţia să incrimineze relatările mele. După ce *New York Times* m-a proclamat „activist", Sullivan a recunoscut că „aceste chestiuni au căpătat o semnificaţie mai mare în climatul actual și ar putea fi cruciale pentru dl. Greenwald".

Aluzia la „climatul actual" era sintagma prin care erau desemnate două controverse majore care afectaseră Washingtonul, implicând tratamentul aplicat de administraţie jurnaliștilor. Prima era obţinerea secretă de către DOJ a datelor de e-mail și telefonice ale reporterilor și redactorilor Associated Press pentru a le afla sursele.

A doua, un incident mai extrem, implica eforturile DOJ de a afla identitatea unei alte surse care fusese la originea

unei scurgeri de informaţii secrete. Pentru a face acest lucru, departamentul depusese un afidavit la curtea federală prin care cerea mandat pentru a citi e-mailurile șefului biroului din Washington al Fox News, James Rosen.

În cererea depusă, avocaţii guvernamentali îl numiseră pe Rosen „participant la conspiraţia“ privind delictele comise de sursă în virtutea faptului că obţinuse materiale secretizate. Afidavitul a fost șocant pentru că, așa cum afirma *New York Times*, „nici un jurnalist nu fusese acuzat vreodată pentru obţinerea și publicarea de informaţii secretizate, așa că această exprimare a deschis perspectiva ca administraţia Obama să ducă represiunea sa împotriva scurgerilor de informaţii la un nou nivel“.[3]

Comportamentul citat de DOJ[4] pentru a justifica desemnarea lui Rosen drept „participant la conspiraţie“ – colaborând cu o sursă pentru a obţine documente, stabilind un „plan de comunicare sub acoperire“ pentru ca aceasta să vorbească fără a fi depistată și „măgulind-o și mizând pe vanitatea și pe ego-ul [sursei sale]“ pentru a o convinge să dezvăluie informaţii – erau toate lucruri pe care jurnaliștii de investigaţii le fac de obicei.

Așa cum afirma reporterul veteran de la Washington Olivier Knox, DOJ l-a „acuzat pe Rosen de încălcarea legii antispionaj printr-un comportament care – așa cum a fost descris în propria declaraţie a agentului – se menţine în limitele activităţii jurnalistice tradiţionale“.[5] Să vezi conduita lui Rosen drept o infracţiune însemna să incriminezi jurnalismul însuși.

Această mișcare a fost poate mai puţin surprinzătoare decât ar fi putut fi, având în vedere contextul mai larg al atacurilor administraţiei Obama la adresa avertizorilor de integritate și a surselor. În 2011, *New York Times* a dezvăluit că DOJ , încercând să găsească sursa unui articol scris de James Rosen, a obţinut „date ample despre apelurile sale telefonice, date financiare și istoricul deplasărilor sale“[6], inclusiv „datele de pe «cardul de credit și cele bancare, precum și unele privind

călătoriile sale cu avionul» și trei desfășurătoare care conţineau conturile sale financiare".

DOJ a încercat, de asemenea, să îl oblige pe Rosen să dezvăluie identitatea sursei prezentându-i perspectiva probabilă a închisorii dacă refuză acest lucru. Jurnaliștii din întreaga ţară au fost îngroziţi de modul în care a fost tratat Rosen: dacă unul dintre reporterii de investigaţie cei mai realizaţi și mai protejaţi instituţional poate fi subiectul unui atac atât de agresiv, atunci acest lucru i se poate întâmpla oricărui jurnalist.

Multe persoane din presă au răspuns alarmate. Un articol tipic, din *USA Today*, menţiona că „președintele Obama este în centrul acuzaţiilor pentru că administraţia sa a lansat efectiv un război împotriva jurnaliștilor"[7] și cita un fost reporter pe securitate naţională al *Los Angeles Times*, Josh Meyer, care afirma: „Există o linie de demarcație pe care nici o administraţie nu a depășit-o până acum înainte de administraţia Obama". Jane Maxer, admiratul reporter de investigații al *New Yorker*, a avertizat în *New Republic* că urmărirea de către DOJ a avertizorilor de integritate reprezintă un atac asupra jurnalismului însuși: „Este un impediment uriaș pentru activitatea jurnalistică și, cum descurajarea nu este suficient de puternică, este mai degrabă un îngheţ al întregului proces într-un punct mort".[8]

Comisia pentru protejarea jurnaliștilor – o organizaţie internaţională care monitorizează atacurile statului asupra libertăţii presei – a fost impresionată de situaţie și a emis primul său raport despre Statele Unite.[9] Scris de Leonard Downie Jr., fost redactor-șef la *Washington Post*, raportul, publicat în octombrie 2013, conchidea:

> Războiul administrației împotriva scurgerilor de informații şi alte eforturi de a controla informația sunt cele mai agresive... de la administrația Nixon... Cei 30 de jurnalişti cu experiență de la Washington de la diferite organizații de presă... intervievați pentru acest raport nu îşi amintesc vreun precedent.

Procesul s-a extins dincolo de securitatea naţională, incluzând, așa cum afirma un șef de birou, un efort de a „zădărnici relatarea responsabilă despre *agenţiile* guvernamentale“.

Jurnaliștii americani, dintre care mulţi au fost fermecaţi ani de zile de Barack Obama, vorbeau acum despre el în mod obișnuit în acești termeni: un fel de ameninţare gravă la adresa libertăţii presei, cel mai represiv lider în această privinţă de la Richard Nixon. Aceasta a fost o turnură remarcabilă pentru un politician care a ajuns la putere promiţând „cea mai transparentă administraţie din istoria SUA“.

Pentru a tempera scandalul care lua amploare, Obama i-a ordonat procurorului general Eric Holder să se întâlnească cu reprezentanţii presei și să revizuiască regulile privind tratamentul DOJ faţă de jurnaliști. Obama a pretins că este „deranjat de posibilitatea ca anchetele privind scurgerile de informaţii să descurajeze jurnalismul de investigaţie care trage la răspundere guvernul“[10] – ca și cum nu ar fi condus timp de cinci ani exact acel tip de atacuri asupra procesului de strângere de informaţii jurnalistice.

Holder a promis într-o audiere în Senat[11] la 6 iunie 2013 (la o zi după primul articol din *Guardian* despre NSA) că DOJ nu va urmări „nici un reporter pentru că își face meseria“. Scopul DOJ, a adăugat el, este pur și simplu să „identifice și să urmărească oficiali guvernamentali care prejudiciază securitatea naţională încălcându-și jurământul, nu să vizeze membri ai presei sau să îi descurajeze să desfășoare activitatea lor esenţială“.

La un anumit nivel, aceasta a fost o evoluţie binevenită: administraţia s-a confruntat, evident, cu suficiente reacţii negative pentru a crea cel puţin o aparenţă de libertate a presei. Dar există o lacună majoră în promisiunea lui Holder: DOJ stabilise, în cazul lui Rosen de la Fox News, că să colaborezi cu sursa pentru a „fura“ informaţii secretizate iese din raza de acţiune a „activităţii de reporter“. Cu toate acestea, garanţia

lui Holder depindea de modul în care DOJ vedea ce este jurnalismul și ce depășește granițele activității jurnalistice legitime.

În acest context, efortul depus de unele personalități media de a mă proiecta în afara „jurnalismului“ – de a insista că ceea ce fac este „activism“, nu activitate jurnalistică, și prin urmare infracțiune – era un lucru potențial periculos.

Primul apel explicit de a fi urmărit a venit de la congresmenul republican de New York Peter King, care fusese președintele subcomisiei pentru terorism din Camera Reprezentanților și convocase audierile abuzive privind amenințarea teroristă venită „din interiorul“ comunității musulmane americane (în mod ironic, King a fost multă vreme un susținător al IRA). King a confirmat pentru Anderson Cooper de la CNN[12] că reporterii care lucrează la articolele despre NSA ar trebui urmăriți penal „dacă știau că este vorba despre informații secretizate... mai ales de o asemenea amploare“. El a adăugat: „Există o obligație morală și legală, cred, împotriva unui reporter care dezvăluie ceva ce ar compromite atât de grav securitatea națională“.

King a clarificat ulterior pentru Fox News[13] că se referă în mod concret la mine:

> Vorbesc despre Greenwald... nu numai că a dezvăluit aceste informații, el a spus că are nume ale agenților şi informatorilor CIA din întreaga lume şi amenință să le dezvăluie. Ultima dată când s-a făcut acest lucru în SUA, am văzut un şef al unei secții CIA ucis în Grecia... Cred că [urmărirea judiciară a jurnaliştilor] ar trebui să fie foarte țintită, foarte selectivă şi cu siguranță o excepție. Dar în acest caz, când ai pe cineva care dezvăluie secrete ca acesta şi amenință să publice şi mai multe, da, trebuie întreprinsă o acțiune legală împotriva lui.

Faptul că am amenințat să public nume de agenți și informatori CIA a fost o minciună sfruntată, fabricată de King. Cu toate acestea, remarcile sale au deschis calea, iar comentatorii s-au îngrămădit. Marc Thiessen de la *Washington Post*, fost scriitor de discursuri pentru Bush care a publicat o carte în

care justifica programul de tortură al SUA, l-a apărat pe King sub titlul: „Da, publicarea de secrete ale NSA este o infracţiune“[14]. Acuzându-mă de „încălcarea legii 18 USC 798, care incriminează publicarea de informaţii secretizate prin dezvăluirea criptografiei guvernamentale sau a comunicaţiilor serviciilor de informaţii“, a adăugat el, „Greenwald a încălcat în mod clar această lege (așa cum a făcut și *The Post*, de fapt, atunci când a publicat detalii secretizate despre programul PRISM al NSA)“.

Alan Dershowitz a mers la CNN și a declarat: „Greenwald – în opinia mea – a comis în mod clar un delict“[15]. Un cunoscut apărător al libertăţilor civile și al libertăţii presei, Dershowitz a spus, cu toate acestea, că relatarea mea „nu este la limita infracționalității – ci chiar în centrul infracționalităţii“.

Corului tot mai mare i s-a alăturat generalul Michael Hayden[16], care a condus NSA și apoi CIA în timpul lui George Bush și a implementat programul ilegal de spionaj fără mandat al agenţiei. „Edward Snowden“, a scris el pentru CNN.com, „se va dovedi probabil cel mai costisitor dezvăluitor de secrete americane din istoria republicii“, și apoi a adăugat că „Glenn Greenwald“ este „mai demn de caracterizarea de către Departamentul de Justiţie ca participant la conspiraţie decât a fost vreodată James Rosen de la Fox“.

Limitat iniţial la personalităţi din rândul dreptei despre care era de așteptat să vadă jurnalismul ca o infracţiune, corul de voci ce ridica problema urmării judiciare a crescut în timpul apariţiei dezonorante la *Meet the Press*.

Casa Albă însăși a lăudat *Meet the Press* drept o emisiune confortabilă pentru figurile politice din DC și alte elite care vor să își transmită mesajul fără prea multe provocări. Programul săptămânal al NBC a fost lăudat de Catherine Martin, fost director de comunicare al vicepreședintelui Dick Cheney, drept „cel mai bun format al nostru“ pentru că Cheney putea să „controleze mesajul“[17]. Apariţia vicepreședintelui la *Meet the Press* a fost o „tactică pe care o foloseam deseori“, a adăugat ea. Într-adevăr, o înregistrare video în care gazda emisiunii, David

Gregory, dansează pe scenă la Dineul corespondenţilor la Casa Albă, stângaci, dar entuziast, în spatele criticatului Karl Rove, a devenit virală pentru că simbolizează atât de viu ceea ce este emisiunea: un loc în care puterea politică merge pentru a fi amplificată și flatată, unde se face auzită doar înţelepciunea convenţională conformistă, unde este permisă doar o gamă limitată de opinii.

Am fost invitat la emisiune în ultimul minut și doar din necesitate. Cu câteva ore înainte apăruse știrea că Snowden plecase din Hong Kong și se afla într-un avion către Moscova, o turnură dramatică a evenimentelor care dominau în mod inevitabil știrile. *Meet the Press* nu avea nici o alternativă decât să analizeze subiectul și, eu fiind una dintre puţinele persoane care luase legătura cu Snowden, am fost chemat la emisiune ca invitat principal.

L-am criticat aspru pe Gregory în ultimii ani și am anticipat un interviu conflictual. Dar nu m-am așteptat să mă întrebe: „În măsura în care l-ai ajutat și instigat pe Snowden, chiar și în actualele lui mișcări, de ce să nu fii dumneata, domnule Greenwald, acuzat de infracţiune?“[18] Erau atât de multe lucruri în neregulă cu întrebarea, încât mi-a luat un minut să procesez ceea ce mă întreba de fapt.

Cea mai izbitoare problemă era numărul de presupuneri fără fundament conţinute de întrebare. Afirmaţia „în măsura în care“ l-am „ajutat și instigat pe Snowden, chiar și în actualele lui mișcări“ nu este ceva diferit de a spune „în măsura în care Gregory și-a ucis vecinii...“ Nu era decât un exemplu izbitor de formulare de tipul „când ai încetat să îţi mai baţi soţia?“

Dar dincolo de absurditatea retorică, un jurnalist de televiziune tocmai acreditase noţiunea că alţi jurnaliști pot și ar trebui să fie acuzaţi pentru că fac jurnalism, o aserţiune extraordinară. Întrebarea lui Gregory implica faptul că orice reporter de investigaţii din Statele Unite care colaborează cu sursele și primește informaţii secretizate este un infractor.

Acestea au fost teoria și climatul care au făcut reporterii de investigaţii atât de precauţi.

În mod predictibil, Gregory m-a descris repetat ca fiind altceva decât „jurnalist". El și-a prefaţat o întrebare afirmând: „Ești un polemist aici, ai un punct de vedere, ești un editorialist". Apoi a anunţat: „Întrebarea cine este jurnalist poate fi discutabilă în funcţie de ceea ce faci".

Dar Gregory nu a fost singurul care a adus aceste argumente. Nici una dintre persoanele invitate la *Meet the Press* pentru a comenta dialogul meu cu Gregory nu a obiectat la faptul că un jurnalist poate fi acuzat pentru că lucrează cu o sursă. Chuck Todd de la NBC a sprijinit această teorie ridicând amenințător „întrebări" în legătură cu ceea ce a numit „rolul" meu în „complot":

> Glenn Greenwald... cât de mult a fost implicat el în complot?... a avut vreun rol dincolo de a fi simplul receptor al acestei informații? Şi va răspunde el la aceste întrebări? Ştiți, este – este – este o chestiune juridică.

O emisiune a CNN, *Reliable Sources*, a dezbătut problema în timp ce pe ecran apărea întrebarea „Ar trebui pus sub acuzare Glenn Greenwald?"[19]

Walter Pincus de la *Washington Post* – care a spionat studenţi americani din străinătate în numele CIA în anii 1960 – a scris un editorial în care sugera că Laura, Snowden și cu mine am operat în cadrul unui complot orchestrat în secret de fondatorul WikiLeaks Julian Assange.[20] Editorialul era plin de atât de multe erori factuale (pe unele le-am demonstrat într-o scrisoare deschisă adresată lui Pincus) încât *The Post* a fost obligat să atașeze o erată neobișnuit de mare, de trei paragrafe, două sute de cuvinte, în care recunoștea multiplele erori.

În propria sa emisiune la CNBC, editorialistul financiar al *New York Times* Andrew Ross Sorkin afirma:

> Mă simt ca şi cum (A) – am eşuat, lăsându-l [pe Snowden] să plece în Rusia. (B) – în mod clar, chinezii ne urăsc suficient pentru a-l lăsa să plece din țară... Şi acum aproape că l-aş aresta pe Glenn Greenwald, jurnalistul care pare că vrea să îl ajute să meargă în Ecuador.[21]

Faptul că un reporter al *Times*, care luptase prin toate mijloacele la Curtea Supremă a SUA pentru a publica Documentele Pentagonului, cerea arestarea mea era un potenţial semn al devotamentului multor jurnaliști din presa consacrată faţă de administraţia SUA: până la urmă, incriminarea jurnalismului de investigaţie va avea un impact grav asupra ziarului și a angajaţilor acestuia. Sorkin și-a cerut ulterior scuze faţă de mine, dar remarcile sale au demonstrat viteza și ușurinţa cu care astfel de afirmaţii câștigă teren.

Din fericire, această opinie a fost departe de a fi unanimă în rândul corpului de presă american. Într-adevăr, spectrul incriminării a determinat mulţi jurnaliști să vină în sprijinul muncii mele, și la multe emisiuni de televiziune de largă audienţă gazdele erau mai interesate de substanţa dezvăluirilor decât de discreditarea celor implicaţi. Multe condamnări ale întrebării lui Gregory au apărut în săptămâna de după interviu. Din partea *Huffington Post*: „Nu ne vine să credem ceea ce tocmai l-a întrebat David Gregory pe Glenn Greenwald“.[22] Toby Harnden, șeful biroului din Washington al britanicului *Sunday Times*, a scris pe Twitter: „Am fost închis în Zimbabweul lui Mugabe pentru «practicarea jurnalismului». Spune David Gregory că și America lui Obama ar trebui să facă la fel?“[23] Numeroși reporteri și editorialiști ai *New York Times*, *The Post* și altele mi-au luat apărarea atât public, cât și privat. Dar oricât de mare ar fi fost sprijinul, acesta nu contracara faptul că reporterii înșiși aprobaseră perspectiva unei prejudicieri legale.

Avocaţi și alţi consilieri au fost de acord că exista un risc real de a fi arestat dacă mă întorceam în Statele Unite. Am încercat

să găsesc o persoană în a cărei judecată aveam încredere și care să îmi spună că acest risc nu există, că era de neconceput ca DOJ să mă pună sub acuzare. Nimeni nu spunea acest lucru. Părerea generală era că DOJ nu va acţiona explicit împotriva mea pentru activitatea jurnalistică, în intenţia de a evita să pară că îi vânează pe jurnaliști. Îngrijorarea era mai degrabă că administraţia va inventa o teorie că presupusele infracţiuni pe care le comisesem erau în afara domeniului jurnalistic. Spre deosebire de Barton Gellman de la *Washington Post*, eu călătorisem la Hong Kong pentru a mă întâlni cu Snowden înainte de publicarea articolelor; vorbisem cu el regulat după ce ajunsese în Rusia și publicasem articole despre NSA ca liber-profesionist în ziare din întreaga lume. DOJ ar fi putut încerca să pretindă că l-am „ajutat și instigat“ pe Snowden în activitatea de scurgere de informaţii sau că am ajutat un „fugar“ să evite justiţia sau că activitatea mea la ziare străine constituie un fel de spionaj.

Mai mult, comentariul meu despre NSA și administraţia SUA a fost în mod deliberat agresiv și sfidător. Administraţia era fără îndoială disperată să pedepsească pe cineva pentru ceea ce fusese numită cea mai prejudicioasă scurgere de informaţii din istoria ţării, dacă nu pentru a atenua furia instituţională, măcar ca mijloc de descurajare a altora. Pe când cel pe care îl voiau cel mai mult se afla sub scutul azilului politic la Moscova, eu și Laura eram a doua opţiune dezirabilă.

Luni întregi, câţiva avocaţi cu contacte la nivel înalt în Departamentul de Justiţie au încercat să obţină asigurări informale că nu voi fi pus sub acuzare. În octombrie, la cinci luni după apariţia primului articol, congresmenul Alan Grayson i-a scris procurorului general Holder, menţionând că persoane politice importante au cerut arestarea mea și că refuzasem o invitaţie de a depune mărturie în faţa Congresului în legătură cu NSA din cauza îngrijorărilor privind o posibilă punere sub acuzare. El și-a încheiat scrisoarea astfel:

> Consider acest lucru regretabil pentru că (1) activitatea jurnalistică nu este o infracțiune; (2) dimpotrivă, ea este protejată explicit prin Primul Amendament; (3) relatările domnului Greenwald despre aceste subiecte ne-au informat de fapt pe mine şi pe alți membri ai Congresului, precum şi publicul larg despre încălcările grave şi generalizate ale legii şi drepturilor constituționale comise de agenți ai administrației.[24]

Scrisoarea întreba dacă Departamentul de Justiţie intenţiona să îmi aducă acuzaţii și dacă, în cazul în care aș încerca să intru în Statele Unite, „Departamentul de Justiţie, Departamentul pentru Securitate Internă sau alte birouri ale administraţiei federale intenţionează să mă reţină, să mă chestioneze, să mă aresteze sau să mă pună sub acuzare". Dar, așa cum relata ziarul din orașul natal al lui Grayson, *Orlando Sentinel*, în decembrie, Grayson nu a primit niciodată răspuns la scrisoare.

La sfârșitul lui 2013 și la începutul lui 2014, ameninţarea cu punerea sub acuzare a crescut, în timp ce oficialii guvernamentali menţineau un atac coordonat pentru a incrimina activitatea mea. La sfârșitul lui octombrie, șeful NSA Keith Alexander, într-o referire evidentă la activitatea mea liber-profesionistă din întreaga lume[25], s-a plâns că „reporterii de ziare au toate aceste documente, cele 50 000 – indiferent ce conțin ele și ce vând" și a cerut ca „noi" – administraţia – „să propunem o modalitate de a pune capăt acestei situaţii". Președintele Comisiei pentru Serviciile de Informaţii din Camera Reprezentanţilor, Mike Rogers, la o audiere din ianuarie, i-a spus în mod repetat directorului FBI James Comey că unii dintre jurnaliști „vând bunuri furate"[26], calificându-i drept „dealeri de bunuri furate" și „hoţi", și apoi a specificat că vorbește despre mine. Când am început să relatez despre spionajul canadian cu Canadian Broadcasting Corporation, purtătorul de cuvânt parlamentar al guvernului de dreapta al lui Stephen Harper m-a denunţat drept un „spion porno"[27] și a acuzat CBC de cumpărarea de la

mine a unor documente furate. În Statele Unite, directorul comunității serviciilor de informații, James Clapper, a început să folosească termenul penal de „complici" pentru a se referi la jurnaliștii care scriu despre NSA.

Cred că probabilitatea arestării după întoarcerea mea în Statele Unite era de 50%, chiar dacă doar din motive de imagine și controversă la nivel internațional. Potențiala pată pe moștenirea lui Obama, ca primul președinte care punea sub urmărire judiciară un jurnalist pentru că face jurnalism, a fost, presupun, suficient de constrângătoare. Dar așa cum demonstra trecutul apropiat, administrația americană era dispusă să facă tot felul de lucruri reprobabile în numele securității naționale, fără să ia în considerare modul în care restul lumii o percepea. Consecințele unei alegeri greșite – să sfârșesc în cătușe și acuzat în baza legilor privind spionajul, pentru a fi judecat de o justiție federală care se dovedise fără rușine deferentă Washingtonului în astfel de probleme – erau prea semnificative pentru a nu le lua în seamă. Eram hotărât să mă întorc în Statele Unite, dar doar după ce înțelegeam mai clar riscul. Între timp, familia mea, prietenii și tot felul de oportunități importante de a vorbi în Statele Unite despre activitatea pe care o desfășuram erau scoase din calcul.

Faptul că avocații și un congresmen consideraseră riscul ca fiind real era extraordinar, o măsură puternică a eroziunii libertății presei. Și faptul că unii jurnaliști se alăturaseră apelului ca activitatea mea să fie tratată drept infracțiune era un triumf remarcabil al propagandei pentru puterile administrației, care se putea baza pe specialiști antrenați să facă treaba în locul său și să echivaleze jurnalismul de investigație critic cu o infracțiune.

Atacurile la adresa lui Snowden au fost, bineînțeles, mult mai virulente. Acestea erau, de asemenea, în mod bizar identice ca temă. Comentatorii principali, care nu știau nimic despre Snowden, au adoptat instantaneu același tip de clișee pentru

a-l înjosi. În câteva ore de la aflarea numelui său au calomniat în serie comportamentul și motivele sale. El nu era mânat de vreo convingere, au spus ei, ci de „narcisism în căutare de glorie".

Gazda *CBS News*, Bob Schieffer, l-a denunţat pe Snowden ca un tânăr „narcisist"[28] care crede că „este mai deștept decât noi ceilalţi". Jeffrey Toobin de la *New Yorker* l-a diagnosticat drept un „narcisist pretențios care merită să fie în închisoare".[29] Richard Cohen de la *Washington Post* a afirmat că Snowden „nu este paranoic; este pur și simplu narcisist"[30], referindu-se la informaţia că Snowden s-a acoperit cu o pătură pentru ca parolele lui de calculator să nu fie înregistrat de camerele de deasupra. Cohen a adăugat, în mod bizar, că Snowden „va rămâne drept varianta masculină a Scufiţei Roșii" și că presupusa lui dorinţă de glorie va fi zădărnicită.

Aceste caracterizări au fost evident ridicole. Snowden era hotărât să dispară din atenţia publică, așa cum spunea, să nu dea interviuri. El a înţeles că presei îi place să personalizeze fiecare poveste și a vrut să păstreze atenţia concentrată pe supravegherea NSA, nu asupra lui. Potrivit propriilor cuvinte, Snowden a refuzat toate invitaţiile media. Zilnic, luni la rând, am primit telefoane și e-mailuri de la aproape fiecare program de televiziune din Statele Unite, personalităţi ale știrilor de televiziune și jurnaliști faimoși, care au pledat pentru șansa de a vorbi cu Snowden. Gazda emisiunii *Today*, Matt Lauer, a sunat de câteva ori pentru a încerca să mă convingă; *60 Minutes* au fost atât de stăruitori în solicitările lor, încât am renunţat să le mai răspund; Brian Williams a trimis câţiva reprezentanţi pentru a-i pleda cauza. Snowden și-ar fi putut petrece toată ziua și toată noaptea la cele mai influente emisiuni de televiziune, cu lumea uitându-se la el, dacă voia să facă acest lucru.

Dar era de neclintit. I-am transmis solicitările și le-a refuzat, pentru a evita să distragă atenţia de la dezvăluiri. Ciudat comportament pentru un narcisist în căutarea gloriei!

Au urmat și alte condamnări ale personalităţii lui Snowden. Editorialistul *New York Times* David Brooks l-a luat în derâdere

pe baza faptului că „nu a reușit să ajungă la colegiu“[31]. Brooks a decretat că Snowden este „ultimul om neinfluențat“, simbolic pentru „valul tot mai mare de neîncredere, răspândire corozivă a cinismului, erodare a structurii sociale și apariţie a unor persoane care sunt atât de individualiste în concepţii, încât nu înţeleg cu adevărat cum să îi unească pe alţii și să urmărească împreună binele comun“.

Pentru Roger Simon de la *Politico*, Snowden era un „ratat“ pentru că „a renunţat la liceu“[32]. Congresmenul democrat Debbie Wasserman Schultz, care este și șef al Convenției Democrate Naţionale, l-a condamnat pe Snowden, care tocmai își distrusese viaţa pentru a face dezvăluiri despre NSA, ca fiind un „laș“[33].

În mod inevitabil, patriotismul lui Snowden a fost pus la îndoială. Pentru că plecase în Hong Kong, s-au făcut afirmaţii că probabil lucra ca spion pentru guvernul chinez. „Nu este greu de imaginat că Snowden a fost agent dublu chinez și că va dezerta curând“[34], a anunţat veteranul consultant de campanie al republicanilor Matt Mackowiak.

Dar atunci când Snowden a plecat din Hong Kong pentru a se îndrepta către America Latină prin Rusia, acuzaţia a fost schimbată brusc din spion chinez în spion rus. Oameni precum congresmenul Mike Rogers au făcut această acuzaţie fără nici o dovadă și în pofida faptului evident că Snowden se afla în Rusia doar pentru că Statele Unite îi anulaseră pașaportul și apoi intimidaseră ţări precum Cuba pentru a revoca promisiunea de trecere sigură. Mai mult, ce fel de spion rus ar merge în Hong Kong sau ar lucra cu jurnaliștii și s-ar legitima public, mai degrabă decât să predea secretele șefilor săi de la Moscova? Afirmaţia era total lipsită de sens și nu se baza pe fapte, dar aceasta nu a împiedicat-o să se răspândească.

Unele dintre cele mai necugetate și nefondate aluzii răspândite împotriva lui Snowden au venit de la *New York Times*, care a pretins că i s-a permis să părăsească Hong Kongul de către guvernul chinez, nu de autorităţile din Hong Kong, și apoi a

adăugat o speculaţie putredă și dăunătoare: „Doi experţi occidentali în servicii de informaţii, care au lucrat pentru agenţii de spionaj guvernamentale majore, au declarat că ei cred că guvernul chinez a reușit să sustragă conţinutul de pe patru laptopuri pe care domnul Snowden le-ar fi adus în Hong Kong“.[35]

New York Times nu avea nici o dovadă că guvernul chinez obţinuse datele NSA ale lui Snowden. Ziarul pur și simplu îndruma cititorii să tragă concluzia că așa a făcut, bazându-se pe doi „experţi“ anonimi care „credeau“ că acest lucru s-ar fi putut întâmpla.

La momentul apariţiei articolului, Snowden era blocat pe aeroportul din Moscova și nu putea intra online. Imediat ce a reapărut, a negat vehement printr-un articol pe care l-am publicat în *Guardian* că a transmis date Chinei sau Rusiei. „Nu am oferit niciodată informaţii vreunui alt guvern, iar ei nu au luat nimic niciodată din laptopurile mele“[36], a declarat el.

La o zi după ce a apărut dezminţirea lui Snowden, Margaret Sullivan a criticat *Times* pentru articol.[37] Ea l-a chestionat pe Joseph Kahn, redactorul Departamentului externe al ziarului, care a declarat că „este importantă această trecere în revistă așa cum este ea: o explorare a ceea ce s-ar fi putut întâmpla, pe baza unor experţi care nu au pretins că au informaţii directe despre acest lucru“. Sullivan a comentat că „două propoziţii din mijlocul articolului *Times* pe un subiect atât de sensibil – deși pot fi în afara punctului central – au puterea de a influenţa discuţia sau de a distruge o reputaţie“. Ea a conchis declarându-se de acord cu un cititor care se plânsese în legătură cu articolul afirmând: „Citesc *Times* pentru a afla adevărul. Pot citi articole despre speculaţii aproape oriunde“.

Prin intermediul lui Janine Gibson, redactorul-șef al *Times* Jill Abramson – la o întâlnire pentru a convinge *Guardian* să colaboreze la unele articole despre NSA – mi-a trimis un mesaj: „Te rog să îi spui personal lui Glenn Greenwald că sunt total de acord cu el în legătură cu faptul că nu ar fi trebuit să publicăm

acea afirmaţie despre sustragerea de către China a informaţiilor din laptopurile lui Snowden. A fost iresponsabil".

Gibson părea să se aștepte să fiu încântat, dar singura mea reacţie a fost: Cum poate un redactor-șef la un ziar să conchidă că un articol în mod evident dăunător a fost iresponsabil și că nu ar fi trebuit publicat și să nu îl retracteze sau cel puţin să scrie o notă?

Dincolo de lipsa de probe, afirmaţia că laptopurile lui Snowden fuseseră „golite" de informații nu are sens în sine. Oamenii nu folosesc laptopurile pentru a transporta cantităţi mari de date ani de zile. Chiar și înainte ca laptopurile să devină ceva comun, documentele erau stocate pe discuri; acum, pe stickuri de memorie. Este adevărat că Snowden a avut patru laptopuri cu el în Hong Kong, folosite pentru scopuri de securitate diferite, dar aceasta nu are nici o legătură cu cantitatea de documente pe care a luat-o cu el. Au fost stickuri criptate prin metode sofisticate. Lucrând ca hacker al NSA, Snowden știa că acestea nu pot fi sparte nici de NSA, ca să nu mai vorbim de agenţiile de spionaj chineze sau ruse.

Invocarea numărului de laptopuri pe care le avea Snowden a fost o modalitate profund derutantă de a se juca cu ignoranţa și temerile oamenilor – *a luat atât de multe documente, încât a avut nevoie de patru laptopuri pentru a le stoca pe toate!* Și chiar dacă chinezii ar fi reușit cumva să sustragă conţinutul, nu ar fi obţinut nimic de valoare.

La fel de fără sens era și ideea că Snowden ar încerca să se salveze predând secrete privind supravegherea. El și-a distrus viaţa și a riscat să fie închis pentru a spune lumii despre sistemul de supraveghere clandestină despre care credea că trebuie oprit. Faptul că s-ar răzgândi ajutând China sau Rusia să își îmbunătăţească propriile capacităţi de supraveghere, pentru a evita închisoarea, era pur și simplu o prostie.

Afirmaţia poate că era fără sens, dar prejudiciul s-a dovedit pe cât de predictibil, pe atât de substanţial. Orice discuţie televizată despre NSA implica invariabil pe cineva care afirma,

fără să fie contrazis, că, acum, China are în posesie, prin intermediul lui Snowden, unele dintre cele mai sensibile secrete ale Statelor Unite. Sub titlul „De ce l-a lăsat China pe Snowden să plece", *New Yorker* le-a spus cititorilor săi că „utilitatea sa era aproape epuizată. Experţi în spionaj citaţi de *Times* credeau că guvernul chinez «a reușit să sustragă conţinutul celor patru laptopuri pe care domnul Snowden a afirmat că le-a adus în Hong Kong»".[38]

Demonizarea personalităţii oricui provoacă puterea politică fusese o tactică deja consacrată folosită de Washington, inclusiv de presă. Unul dintre primele și poate cel mai elocvent exemplu al acestei tactici a fost tratamentul administraţiei Nixon faţă de avertizorul de integritate Daniel Ellsberg, care a fost la originea publicării Documentelor Pentagonului, ce a inclus spargerea biroului psihanalistului lui Ellsberg pentru a fura dosarele lui Ellsberg și a căuta detalii despre viaţa sa sexuală. Oricât de lipsită de sens ar părea această tactică – de ce dezvăluirea unor informaţii personale stânjenitoare ar contracara dovada înșelăciunii administraţiei –, Ellsberg a înţeles clar: oamenii nu vor să fie asociaţi cu cineva care a fost discreditat și umilit public.

Aceeași tactică a fost folosită pentru a prejudicia reputaţia lui Julian Assange cu mult înainte ca el să fie acuzat de abuz sexual de două femei din Suedia. Evident, atacuri la adresa lui Assange au fost desfășurate de aceleași ziare care au colaborat cu el și au beneficiat de dezvăluirile lui Chelsea Manning pe care Assange și WikiLeaks le publicaseră.

Când *New York Times* a publicat ceea ce a numit „Jurnalele războiului din Irak" – mii de documente secretizate detaliind atrocităţile și alte abuzuri din timpul războiului comise de armata SUA și de aliaţii săi în Irak –, ziarul a prezentat un articol de prima pagină – la fel de remarcabil ca dezvăluirile – scris de reporterul prorăzboi John Burns, care nu avea alt scop decât să îl descrie pe Assange drept ciudat și paranoic, cu un contact redus cu realitatea.

Articolul descrie cum Assange „s-a cazat la hoteluri sub nume false, și-a vopsit părul, a dormit pe canapele și podele și a folosit bani lichizi în loc de carduri de credit, adeseori împrumutaţi de la prieteni“.[39] Acesta a menţionat ceea ce a numit „un comportament dezordonat și arogant“ și „iluzia grandorii“ și a afirmat că oponenții săi „îl acuză că urmărește o vendetă împotriva Statelor Unite“. Mai mult, a adăugat acest diagnostic psihologic din partea unui voluntar WikiLeaks nemulţumit: „Nu este în toate minţile“.

Prezentarea lui Assange drept nebun și delirant a devenit o marcă a discursului politic american în general și a tacticilor *New York Times* în special. Într-un articol, Bill Keller a citat un reporter al *Times* care l-a descris pe Assange ca „neîngrijit, ca o cerșetoare care colindă străzile, purtând o haină sport decolorată și murdară și pantaloni cu buzunare, un tricou alb murdar, tenişi uzaţi și șosete albe murdare căzute în jurul gleznelor. Mirosea de parcă nu se spălase cu zilele“.[40]

Times a condus și relatările despre Manning, insistând că ceea ce l-a determinat pe Manning să devină un avertizor de integritate nu a fost convingerea sau conștiinţa, ci problemele de personalitate și instabilitatea psihică. Numeroase articole au speculat, fără nici un fundament, că totul, de la luptele împotriva intimidării antigay din armată la conflictele cu tatăl său, a constituit motive principale în decizia sa de a dezvălui documente atât de importante.

Explicarea disidenţei prin probleme de personalitate este departe de a fi o invenţie americană. Disidenţii sovietici erau internaţi în mod obișnuit în spitale psihiatrice, iar cei chinezi încă sunt trataţi în mod forţat de boli psihice. Există motive evidente pentru a lansa atacuri personale la adresa celor care critică starea de fapt. Așa cum am menţionat, unul este de a face criticile mai puţin eficiente: puţine persoane vor să se asocieze cu cineva nebun sau ciudat. Altul este descurajarea: când disidenţii sunt descriși de societate și înjosiţi ca instabili emoţional, ceilalţi sunt puternic stimulaţi să nu devină ca ei.

Dar principalul motiv este necesitatea logică. Pentru gardienii statu-quo-ului nu există nimic pur sau fundamental greșit cu ordinea prevalentă și instituţiile sale dominante, care sunt considerate juste. Prin urmare, oricine pretinde altceva – în special cineva suficient de motivat de acea credinţă încât să adopte o acţiune radicală – trebuie, prin definiţie, să fie instabil emoţional și cu probleme psihice.

Cu alte cuvinte, există, la drept vorbind, două alegeri: obedienţa faţă de autoritatea instituţională sau disidenţa radicală. Prima este o alegere sănătoasă și validă doar dacă a doua este smintită și ilegitimă. Pentru apărătorii statu-quo-ului, principala *corelaţie* între boala mintală și opoziţia radicală pentru prevalenţa dogmei este insuficientă. Disidenţa radicală este o evidenţă, chiar o dovadă, a unei tulburări severe de personalitate.

În centrul acestei formulări stă o eroare esenţială: această disidenţă faţă de autoritatea instituţională implică o alegere morală sau ideologică, în timp ce obedienţa nu implică acest lucru. Cu această falsă premisă, societatea acordă o mare atenţie motivelor disidenţilor, dar nici una celor care se supun instituţiilor, fie asigurându-se că acţiunile lor rămân ascunse, fie folosind alte metode. Obedienţa faţă de autoritate este implicit considerată starea naturală.

De fapt, atât respectarea, cât și încălcarea legilor implică alegeri morale, și ambele cursuri ale acţiunii dezvăluie ceva important despre individul implicat. Dimpotrivă, acceptarea premisei – disidenţa radicală demonstrează o tulburare de personalitate – înseamnă că opusul poate fi adevărat: în faţa unei nedreptăţi grave, refuzul de a nu fi de acord este semnul unui defect de caracter sau al unui eșec moral.

Profesorul de filosofie Peter Ludlow, scriind în *New York Times* despre ceea ce numește „scurgerea de informaţii, avertizarea de integritate și hacktivismul care au ofensat armata SUA și comunităţile de informaţii private și guvernamentale“[41] – activităţi sociale asociate cu un grup pe care el îl

numește „Generaţia W“, cu Snowden și Manning ca exemple principale – subliniază exact acest lucru:

> Dorința presei de a psihanaliza membrii generației W este destul de naturală. Ei vor să ştie de ce aceste persoane acționează într-un fel în care ei, membri ai presei corporatiste, nu ar face-o. Dar ce este acceptabil pentru unii nu este pentru alții; dacă există motivații psihologice pentru avertizarea de integritate, scurgerea de informații şi hacktivism, există motivații psihologice şi pentru strângerea rândurilor în jurul structurii puterii în cadrul unui sistem – în acest caz un sistem în care mass-media corporatistă joacă un rol important.
>
> În mod similar, este posibil ca însuşi sistemul să fie bolnav, chiar dacă actorii din cadrul organizației se comportă în acord cu eticheta organizațională şi respectă legăturile interne de încredere.

Această discuţie este una pe care autorităţile instituţionale sunt foarte dornice să o evite. Demonizarea recurentă a avertizorilor de integritate este o modalitate prin care presa consacrată din Statele Unite protejează interesele celor care deţin puterea. Atât de profundă este supunerea, încât multe reguli ale jurnalismului sunt croite sau cel puţin aplicate astfel încât să promoveze mesajul guvernului.

Să luăm, de exemplu, noţiunea că scurgerea de informaţii secretizate este un fel de act rău intenţionat sau criminal. De fapt, jurnaliștii de la Washington care ne-au aplicat această etichetă, lui Snowden sau mie, nu deplâng toate scurgerile de informaţii secrete, ci doar pe cele a căror dezvăluire displace sau subminează administraţia.

Realitatea este că Washingtonul este mereu implicat în scurgeri de informaţii. Cei mai celebri și mai veneraţi reporteri din DC, precum Bob Woodward, și-au asigurat poziţia primind în mod obișnuit informaţii secretizate din partea unor surse de la nivel înalt și apoi publicându-le. Oficialii lui Obama au mers în mod repetat la *New York Times* pentru a distribui informaţii

secretizate despre subiecte precum uciderea cu drone și asasinarea lui Osama bin Laden. Fostul secretar al apărării Leon Panetta și oficiali din cadrul CIA i-au oferit informații secrete regizoarei *Zero Dark Thirty**, sperând că filmul va trâmbița cel mai mare triumf politic al lui Obama. (În același timp, avocați ai Departamentului de Justiție au declarat tribunalelor federale că, pentru a proteja securitatea națională, nu vor publica informații despre raidul care l-a vizat pe bin Laden.)

Nici un jurnalist consacrat nu va propune urmărirea judiciară a vreunuia dintre oficialii responsabili de aceste scurgeri de informații sau a reporterilor care le primesc și scriu despre ele. Ar râde la sugestia ca Bob Woodward, care a publicat secrete importante ani la rând, și sursele sale guvernamentale de rang înalt să fie incriminați.

Aceasta pentru că respectivele scurgeri de informații sunt aprobate de Washington și servesc intereselor administrației SUA, motiv pentru care sunt considerate adecvate și acceptabile. Singura scurgere de informații pe care mass-media de la Washington o condamnă este aceea care conține informații pe care oficialii ar prefera să le ascundă.

Să analizăm ce s-a întâmplat cu puțin timp înainte ca David Gregory să sugereze la *Meet the Press* ca eu să fiu arestat pentru relatările despre NSA. La începutul interviului, m-am referit la o decizie judiciară strict secretă emisă de tribunalul FISA în 2011, care considera părți substanțiale din programul de supraveghere internă al NSA drept neconstituționale și ca încălcând statutele care reglementează spionajul. Știam despre această decizie doar pentru că citisem despre ea în documentele NSA pe care Snowden mi le dăduse. La *Meet the Press*, cerusem publicarea sa.

Totuși, Gregory a considerat de cuviință să afirme că FISA emisese o altă concluzie:

---

* *Misiunea: 0.30 A.M.* – film din 2012 al regizoarei Kathryn Bigelow, nominalizat la Premiile Oscar (n.red.)

> Potrivit persoanelor cu care am discutat, acea concluzie FISA bazată pe solicitarea administrației demonstrează că ei spun, „bine, puteți asta, dar nu puteți cealaltă. Aceasta ar depăşi de fapt sfera de acțiune a ceea ce ți se permite să faci“ – ceea ce înseamnă că solicitarea a fost schimbată sau respinsă, iar asta e tot ce punctează administrația, şi anume că există o revizuire judiciară aici, şi nu un abuz.[42]

Importante aici sunt detaliile concluziei tribunalului FISA (deși atunci când a fost publicată, opt săptămâni mai târziu, a devenit clar că decizia a conchis într-adevăr că NSA acţionase ilegal). Mai important este că Gregory pretindea că știe despre decizie pentru că sursele sale îi spuseseră despre ea și apoi el a difuzat informaţia lumii întregi.

În aceste momente dinainte ca Gregory să aducă în discuţie arestarea mea pentru relatări, el însuși a difuzat ceea ce credea că este o informaţie strict secretă din surse guvernamentale. Dar nimeni nu a sugerat vreodată că Gregory ar trebui incriminat. Aplicarea aceluiași raţionament gazdei *Meet the Press* și sursei sale ar fi considerată ridicolă.

Într-adevăr, Gregory ar fi probabil incapabil să înţeleagă că dezvăluirea făcută de el și cea făcută de mine sunt comparabile în vreun fel, de vreme ce a lui a venit în numele solicitării administraţiei de a apăra și justifica acţiunile sale, în timp ce a mea a fost făcută în mod critic, împotriva voinţei oficialităţilor.

Aceasta este, bineînţeles, exact opusul a ceea ce ar trebui să realizeze libertatea presei. Ideea de a „patra putere“ este că aceia care exercită cea mai mare putere trebuie provocaţi prin critici și insistenţa pe transparenţă; treaba presei este să dezaprobe falsurile pe care puterea le distribuie invariabil pentru a se proteja. Fără acest tip de jurnalism, abuzul este inevitabil. Nimeni nu are nevoie ca libertatea presei să fie garantată de Constituţia SUA pentru ca jurnaliștii să fie prietenoși și să glorifice liderii politici; garanţia a fost necesară tocmai pentru ca jurnaliștii să poată face contrariul.

Dublul standard aplicat publicării informaţiilor secretizate este și mai pronunţat atunci când vine vorba despre solicitările nescrise de „obiectivitate jurnalistică". Presupusa încălcare a acestei norme este cea care m-a făcut un „activist" mai degrabă decât un „jurnalist". Așa cum ni se spune la nesfârșit, jurnaliștii nu exprimă opinii; ei pur și simplu relatează fapte.

Aceasta este evident o scuză, o vanitate a profesiei. Percepţiile și exprimările fiinţelor umane sunt inerent subiective. Fiecare articol este produsul a tot felul de presupuneri culturale, naţionaliste și politice profund subiective. Și tot jurnalismul servește interesului unei facţiuni sau al alteia.

Distincţia relevantă nu este între jurnaliști care au opinii și cei care nu au, o categorie care nu există. Ci este între jurnaliști care își dezvăluie sincer opiniile și cei care și le ascund, pretinzând că nu au unele.

Însăși ideea că reporterii ar trebui să nu aibă opinii este departe de cerinţele tradiţionale ale profesiei; de fapt, este o născocire relativ nouă care a avut efectul, dacă nu intenţia, de a neutraliza jurnalismul.

Această viziune americană recentă reflectă, așa cum a remarcat Jack Shafer, editorialist Reuters, un „devotament trist faţă de idealul corporatist privitor la ceea ce jurnalismul" ar trebui să fie, precum și „o lipsă dureroasă de înţelegere istorică"[43]. De la fondarea Statelor Unite, cel mai bun și mai semnificativ jurnalism a implicat frecvent reporteri combativi, militantism și devotament pentru lupta împotriva nedreptăţii. Șablonul fără opinie, fără culoare, fără suflet al jurnalismului corporativ a secat meseria de cele mai valoroase atribute ale sale, făcând presa consacrată nesemnificativă: o ameninţare la adresa cuiva fără putere, exact cum s-a intenţionat.

Dar dincolo de amăgirea inerentă a relatării obiective, regula nu este aproape niciodată aplicată de cei care pretind că ei cred în ea. Jurnaliștii consacraţi își exprimă constant opiniile într-o serie de probleme controversate fără să le fie negat statutul profesional. Dar dacă opiniile pe care le exprimă ei sunt

aprobate de oficialităţile de la Washington, ei sunt percepuţi ca legitimi.

De-a lungul controversei privind NSA, Bob Schieffer, gazda emisiunii *Face the Nation*, l-a denunţat pe Snowden și a apărat supravegherea NSA, așa cum a făcut și Jeffrey Toobin, corespondent pe justiţie al *New Yorker* și CNN. John Burns, corespondentul *New York Times* care a scris despre războiul din Irak, a recunoscut ulterior că a susţinut invazia, descriind trupele americane chiar ca „eliberatorii mei" și „îngeri păzitori". Christiane Amanpour de la CNN și-a petrecut vara lui 2013 militând pentru folosirea forţei militare americane în Siria. Aceste poziţii nu au fost condamnate însă ca „activism" – cu toată veneraţia faţă de obiectivitate, nu există de fapt nici o prevedere care să le interzică jurnaliștilor să aibă opinii.

La fel ca presupusa regulă împotriva scurgerii de informaţii, „regula" obiectivităţii nu este deloc o regulă, ci mai degrabă un mijloc de promovare a intereselor clasei politice dominante. Prin urmare, „supravegherea NSA este legală și necesară" sau „războiul din Irak este corect" sau „Statele Unite ar trebui să invadeze acea ţară" sunt opinii acceptabile pe care jurnaliștii le pot exprima, și ei fac acest lucru tot timpul.

„Obiectivitatea" nu înseamnă altceva decât reflectarea prejudecăţilor și servirea intereselor înrădăcinate la Washington. Opiniile sunt problematice doar atunci când deviază de la linia acceptată a dogmei Washingtonului.

Ostilitatea faţă de Snowden nu este greu de explicat. Ostilitatea faţă de un reporter care prezintă știrea – adică faţă de mine – este poate mai complexă. Parţial din competiţie, parţial din răzbunare pentru anii de critică profesională a starurilor mass-media americane, a fost, cred, și o furie și chiar o rușine faţă de adevărul pe care jurnalismul critic l-a dezvăluit: relatări care înfurie administraţia dovedesc rolul real al atâtor jurnaliști de prim-plan, acela de a amplifica puterea.

Dar de departe cel mai semnificativ motiv al ostilităţii a fost că figuri ale mass-media consacrate acceptaseră regula

purtătorilor de cuvânt ascultători ai oficialilor politici, mai ales atunci când este vizată securitatea naţională. Prin urmare, reiese că la fel ca oficialii înșiși, ei sunt dispreţuitori faţă de cei care provoacă sau subminează centrele de putere de la Washington.

Reporterul tipic din trecut era outsiderul definitiv. Mulţi dintre cei care au intrat în profesie erau înclinaţi să se opună mai degrabă decât să servească puterea, nu numai prin ideologie, ci și prin personalitate și dispoziţie. Alegerea unei cariere în jurnalism asigura practic un statut de outsider: reporterii făceau bani puţini, aveau prestigiu instituţional scăzut și erau în general necunoscuţi.

Acest lucru s-a schimbat acum. Odată cu achiziţionarea companiilor de presă de către cele mai mari corporaţii ale lumii, majoritatea vedetelor mass-media sunt angajaţi foarte bine plătiţi ai unor conglomerate, fără vreo diferenţă faţă de alt tip de angajaţi. În loc să vândă servicii bancare sau instrumente financiare, ei vând produse media publicului în numele corporaţiei. Cariera lor este determinată de aceleași caracteristici care duc la succes într-un astfel de mediu: măsura în care ei le fac pe plac șefilor corporatiști și promovează interesele companiei. Cei care prosperă în cadrul structurii marilor corporaţii tind să fie adepţii satisfacerii mai degrabă decât ai răsturnării puterii instituţionale. Reiese că aceia care au succes în jurnalismul corporatist sunt obișnuiţi să se adapteze puterii. Ei se identifică cu autoritatea instituţională și sunt iscusiţi în a o servi, nu în a o combate.

Dovezile sunt multe. Știm despre dorinţa *New York Times* de a interzice publicarea, la comanda Casei Albe, a descoperirii lui James Risen privind programul de interceptări ilegale al NSA din 2004; redactorul responsabil cu normele de etică al ziarului la vremea respectivă a descris scuzele publicaţiei de interzicere drept „deplorabil de inadecvate“[44]. Într-un incident similar la *Los Angeles Times*, redactorul Dean Baquet[45] a omorât un subiect în 2006 al reporterilor săi despre o colaborare

secretă între AT&T și NSA, pe baza informaţiilor oferite de avertizorul de integritate Mark Klein. El a venit cu teancuri de documente pentru a dezvălui construirea de către AT&T a unei încăperi secrete în biroul său din San Francisco, unde NSA putea să instaleze splittere pentru a redirecţiona apelurile telefonice și traficul de internet de la clienţi către bazele de stocare ale agenţiei.

Așa cum afirma Klein, documentele au arătat că NSA „răscolea prin vieţile personale a milioane de americani nevinovaţi“. Dar Baquet a blocat publicarea articolului, a povestit Klein în 2007 pentru *ABC News*, „la cererea directorului de atunci al serviciului de informaţii interne John Negroponte și a directorului de atunci al NSA generalul Michael Hayden“. La scurt timp după aceea, Baquet a devenit șeful din Washington al *New York Times* și apoi a fost promovat în poziţia de redactor coordonator al ziarului.

Faptul că *Times* avansează atât de rapid un servitor al intereselor guvernamentale nu ar trebui să fie o surpriză. Margaret Sullivan, redactor responsabil cu normele de etică al ziarului, menţiona[46] că *Times* poate ar trebui să se uite în oglindă dacă redactorii săi vor să înţeleagă de ce sursele care dezvăluie subiecte majore de securitate naţională, precum Chelsea Manning și Edward Snowden, nu se simt în siguranţă sau motivate să le ofere lor informaţia. Este adevărat că *New York Times* a publicat documente importante în parteneriat cu WikiLeaks, dar, la scurt timp după aceea, fostul redactor-șef Bill Keller s-a străduit să distanţeze ziarul de partenerul său: el a comparat public furia administraţiei Obama împotriva WikiLeaks cu aprecierile la adresa *Times* și a activităţii sale „responsabile“.

Keller a trâmbiţat mândru relaţia ziarului său cu Washingtonul și cu alte ocazii. Într-o apariţie la BBC în 2011 în care discuta despre telegramele obţinute de WikiLeaks, Keller a explicat că *Times* primește instrucţiuni de la administraţia SUA în legătură cu ce ar trebui și cu ce nu ar trebui să publice.

Moderatorul BBC l-a întrebat incredul: „Spuneţi că mergeţi la administraţie înainte și întrebaţi: «Ce părere aveţi despre una, alta sau celelalte, este în regulă să facem asta sau asta» și primiţi apoi undă verde?“.[47] Celălalt invitat, ambasadorul britanic Carne Ross, a declarat că afirmaţiile lui Keller l-au făcut să se gândească ulterior că nu ar trebui să mergi la *New York Times* pentru aceste telegrame. „Este extraordinar că *New York Times* stabilește cu administraţia SUA ce spune despre acest lucru.“

Dar nu este nimic extraordinar în legătură cu acest tip de colaborare cu Washingtonul. Este ceva obișnuit, de exemplu, pentru reporteri să adopte poziţia oficială a SUA în disputele cu adversarii străini și să ia decizii editoriale pe baza a ceea ce promovează mai bine „interesele SUA“, așa cum sunt ele definite de administraţie. Avocatul DOJ din administraţia Bush Jack Goldsmith a lăudat ceea ce el a numit „un fenomen subapreciat: patriotismul presei americane“[48], însemnând că presa internă tinde să demonstreze loialitate agendei guvernamentale. El l-a citat pe directorul CIA și NSA din perioada Bush, Michael Hayden, care a menţionat că jurnaliștii americani dau dovadă de „disponibilitatea de a lucra cu noi“, dar presa străină, a adăugat el, „este foarte, foarte dificilă“.

Această identificare a presei americane cu administraţia este cimentată de diverși factori, unul dintre ei fiind cel socioeconomic. Mulţi jurnaliști influenţi din Statele Unite sunt acum multimilionari. Ei trăiesc în aceleași cartiere cu oamenii politici și elita financiară pentru care servesc în mod evident drept câini de pază. Au aceleași funcţii, aceleași cercuri de prieteni și de cunoscuţi, iar copiii lor merg la aceleași școli private de elită.

Acesta este unul dintre motivele pentru care jurnaliștii și oficialii guvernamentali pot face schimb de locuri de muncă fără probleme. Platforma rotativă împinge personalităţile din presă în funcţii de rang înalt de la Washington, la fel cum oficiali guvernamentali deseori părăsesc funcţia pentru a onora un contract media profitabil. Jay Carney și Richard Stengel de la

revista *Time* sunt acum în administraţie, în timp ce consilierii lui Obama David Axelrod și Robert Gibbs sunt comentatori pentru MSNBC. Acestea sunt transferuri laterale ce depășesc o schimbare de carieră: schimbul este atât de eficientizat tocmai pentru că personalul servește aceleași interese.

Jurnalismul american consacrat este orice altceva, dar nu o forţă outsider. Este pe deplin integrat puterii politice dominante a naţiunii. Din punct de vedere cultural, emoţional și socioeconomic, ei sunt unii și aceiași. Jurnaliștii bogaţi, faimoși din interior nu vor să submineze statu-quo-ul care îi recompensează atât de extravagant. Ca toţi curtenii, ei sunt dornici să apere sistemul care îi investește cu privilegii și sunt dispreţuitori faţă de oricine contestă acest sistem.

Mai este un pas mic până la identificarea deplină cu nevoile oficialilor politici. Prin urmare, transparenţa nu este bună; jurnalismul critic este rău; posibil infracţional. Liderilor politici trebuie să li se permită să exercite puterea în întuneric.

În septembrie 2013, aceste puncte erau puternic subliniate de Seymour Hersh, reporter câștigător al Premiului Pulitzer care a dezvăluit atât masacrul My Lai, cât și scandalul Abu Ghraib. Într-un interviu acordat *Guardian*, Hersh s-a raliat împotriva a ceea ce el a numit „timiditatea jurnaliștilor din America, eșecul lor de a contesta Casa Albă și de a fi mesageri ai adevărului“[49]. El a afirmat că *New York Times* petrece prea mult timp „servind intereselor lui Obama“. Administraţia minte sistematic, a afirmat el, „cu toate acestea, nici unul dintre monștrii presei americane, reţelele de televiziune sau titlurile mari din presa scrisă“ nu prezintă o provocare.

Propunerea lui Hersh „în legătură cu modalitatea în care poate fi restabilit jurnalismul“ a fost „închiderea birourilor de știri ale NBC și ABC, concedierea a 90% dintre redactori și revenirea la activitatea fundamentală a jurnaliștilor“, aceea de a fi niște outsideri. „Începerea promovării redactorilor care nu pot fi controlaţi“, a susţinut Hersh. „Scandalagiii nu sunt promovaţi“, a spus el. În schimb, „redactorii lași“ și jurnaliștii

distrug profesia pentru că mentalitatea larg răspândită este să nu îndrăznească să fie niște outsideri.

Odată ce reporterii sunt etichetaţi drept activiști, odată ce munca lor este pătată de acuzaţia de activitate infracţională și sunt scoși din cercul protecţiei acordate jurnaliștilor, ei sunt vulnerabili la un tratament penal. Aceasta s-a întâmplat cu mine la foarte scurt timp după apariţia subiectului NSA.

La câteva minute după ce m-am întors la Rio după șederea la Hong Kong, David mi-a spus că laptopul lui se evaporase. Suspectând că dispariţia avea legătură cu discuţia noastră când eu eram plecat, el mi-a reamintit că îl sunasem pe Skype pentru a vorbi despre un fișier mare, criptat de documente pe care intenţionam să îl trimit electronic. I-am spus că după ce ajunge la el ar trebui să îl pună într-un loc sigur. Snowden considerase vital ca o persoană în care eu am încredere deplină să aibă un set complet de documente, în cazul în care propria noastră arhivă se va pierde, va fi distrusă sau furată.

„Aș putea să nu fiu disponibil multă vreme", a spus el. „Și nu știi niciodată cum va evolua relaţia ta profesională cu Laura. Cineva trebuie să aibă un set la care să ai acces permanent, indiferent ce se întâmplă."

Alegerea evidentă a fost David. Dar nu am trimis niciodată fișierul. A fost unul dintre lucrurile pentru care nu am avut timp cât am stat în Hong Kong.

„La mai puţin de 48 de ore după ce mi-ai spus acest lucru", a spus David, „laptopul meu a fost furat din casă".

Am respins ideea că furtul laptopului avea legătură cu discuţia noastră pe Skype. I-am spus lui David că sunt hotărât ca noi să nu devenim niște persoane paranoice care atribuie CIA orice eveniment inexplicabil din vieţile lor. Poate că laptopul s-a pierdut sau cineva care venise în vizită l-a luat sau poate că a fost furat în timpul unui jaf fără nici o legătură cu activitatea mea.

David a contracarat teoriile mele una câte una: el nu a scos niciodată laptopul din casă; a întors casa cu susul în jos și nu l-a găsit; nimic altceva nu fusese luat sau deranjat. Eram iraţional, credea el, refuzând să susţin ceva ce părea singura explicaţie.

În acel moment, numeroși reporteri menţionaseră că NSA nu avea nici o idee ce luase Snowden sau ce îmi dăduse mie, nu numai documente specifice, dar nici cantitatea lor. Era normal ca administraţia SUA (sau poate alte guverne) să fie disperate să afle ce am. Dacă luarea computerului lui David le oferea informaţii, de ce să nu îl fure?

Știam, de asemenea, că o conversaţie cu David pe Skype nu este deloc sigură, fiind vulnerabilă la monitorizarea NSA la fel ca orice altă formă de comunicare. Așa că administraţia a putut să afle că plănuiam să îi trimit documente lui David, ceea ce îi oferea un motiv puternic pentru a-i lua laptopul.

Am aflat de la David Schultz, avocatul *Guardian*, că există motive să cred teoria lui David privind furtul. Contactele din comunitatea de informaţii americană îi transmiseseră că prezenţa CIA este mai puternică la Rio decât oriunde în altă parte a lumii și că șeful secţiei din Rio este „cunoscut ca agresiv“. Pe baza acestor date, Schultz mi-a spus: „Ar trebui să îţi asumi în mare măsură că tot ceea ce spui, tot ceea ce faci și toate mișcările îţi sunt atent monitorizate“.

Am acceptat că posibilitatea mea de a comunica va fi puternic restricţionată. M-am abţinut de la folosirea telefonului în alt scop decât conversaţii vagi și banale. Am trimis și am primit e-mailuri doar prin greoaiele sisteme de criptare. Am limitat discuţiile mele cu Laura, Snowden și diverse surse la programe de chat online criptate. Am putut să lucrez la articole cu redactorii *Guardian* și cu alţi jurnaliști doar când ei cu călătorit la Rio pentru a ne întâlni faţă în faţă. Am manifestat chiar precauţie în discuţiile cu David în casa sau mașina noastră. Furtul laptopului mi-a arătat clar posibilitatea ca până și cele mai intime spaţii să fie supravegheate.

Dacă mai aveam nevoie de vreo altă dovadă a climatului amenințător în care lucram acum, aceasta a venit sub forma relatării unei conversații surprinse de Steve Clemons, un analist politic bine conectat și bine văzut în DC și colaborator la *Atlantic*.

În 8 iunie, Clemons se afla pe aeroportul Dulles în spațiul destinat United Airlines și povestea că a surprins discuția unor oficiali din cadrul serviciilor de informații americane care afirmau cu voce tare că denunțătorul și reporterul care s-a ocupat de dezvăluirile NSA ar trebui să „dispară". El a spus că a înregistrat o parte din conversația lor pe telefon. Clemons credea că discuția era doar o „bravadă", dar a decis să o publice.

Nu am luat prea în serios povestea, deși Clemons este destul de credibil. Însă simplul fapt că existau astfel de discuții publice inutile în rândul unor indivizi din aparatul de stat despre „dispariția" lui Snowden – și a jurnaliștilor cu care a lucrat – era alarmant.

În lunile care au urmat, posibila incriminare a relatării despre NSA a devenit dintr-o idee abstractă – realitate. Această schimbare drastică a fost inițiată de guvernul britanic.

Am auzit prima dată de la Janine Gibson, printr-o discuție criptată, despre un eveniment remarcabil care avusese loc la biroul *Guardian* din Londra la jumătatea lui iulie. Ea a descris ceea ce a numit o „schimbare radicală" a tonului discuției dintre *Guardian* și GCHQ care avusese loc în ultimele câteva săptămâni. Ceea ce inițial fusese „o discuție foarte civilizată" despre relatarea făcută de ziar a degenerat într-o serie de solicitări tot mai belicoase și apoi amenințări directe din partea agenției britanice de spionaj.

Apoi, mai mult sau mai puțin brusc, mi-a spus Gibson, GCHQ a anunțat că nu va mai „permite" ziarului să continue să publice subiecte pe baza unor documente strict secrete. Ei au cerut ca *Guardian* din Londra să predea toate copiile fișierelor primite de la Snowden. Dacă *Guardian* refuza, un ordin judecătoresc ar fi interzis orice relatare ulterioară.

Amenințarea nu era fără temei. Marea Britanie nu are garanții constituționale pentru libertatea presei. Tribunalele britanice sunt atât de deferente solicitărilor guvernamentale de „prior restraint“ [cenzură înainte de publicare] încât presei i se poate interzice în avans să publice un subiect despre care se consideră că ar amenința securitatea națională.

Într-adevăr, în anii 1970, reporterul care a descoperit și apoi a relatat despre existența GCHQ, Duncan Campbell, a fost arestat și trimis în judecată. În Marea Britanie tribunalele ar fi putut închide *Guardian* în orice moment și ar fi putut confisca toate materialele și echipamentele sale. „Nici un judecător nu ar spune nu dacă i s-ar cere acest lucru“, a zis Janine. „Știm acest lucru și ei știu că noi știm.“

Documentele pe care le deținea *Guardian* erau doar o parte din arhiva pe care Snowden o predase la Hong Kong. El a simțit că relatările despre GCHQ ar trebui făcute de jurnaliști britanici, iar în una dintre ultimele zile la Hong Kong i-a dat o copie a acestor documente lui Ewen MacAskill.

Am sunat-o pe Janine și mi-a spus că ea și redactorul-șef Alan Rusbridger, împreună cu alți membri ai conducerii, fuseseră cu un weekend înainte într-un refugiu dintr-o zonă izolată din afara Londrei. Brusc au auzit că oficialii GCHQ sunt pe drum către redacția *Guardian* din Londra, unde intenționează să confiște hard diskurile pe care erau stocate documentele. „V-ați distrat destul“, i-au spus ei lui Rusbridger, așa cum a povestit el ulterior, „acum ne vrem lucrurile înapoi“. Grupul era la țară de doar două ore și jumătate înainte să afle despre GCHQ. „A trebuit să ne întoarcem la Londra pentru a apăra clădirea. A fost foarte dificil“, a spus Janine.

GCHQ a cerut ca *Guardian* să predea toate copiile arhivei. Dacă ziarul se conforma, guvernul ar fi aflat ce transmisese Snowden și poziția sa legală putea fi periclitată. În schimb, *Guardian* a fost de acord să distrugă toate hard diskurile relevante sub privirile oficialilor GCHQ. Ce s-a întâmplat a fost, potrivit descrierii lui Janine, „un dans foarte elaborat

de rezistență, diplomație, contrabandă și apoi «distrugere demonstrabilă» cooperantă".

Termenul „distrugere demonstrabilă" era nou inventat de GCHQ pentru a descrie ceea ce avusese loc. Oficialii au însoțit personalul *Guardian*, inclusiv pe redactorul-șef, în subsolul redacției și au privit cum aceștia distrugeau hard diskurile, cerându-le chiar să spargă în mod specific anumite părți „doar pentru a fi siguri că nu mai este nimic din bucățile de metal deformate care ar putea fi de vreun interes pentru a fi transmis agenților chinezi", a povestit Rusbridger. „Putem chema elicopterele negre", a povestit el că a glumit un expert în securitate, în timp ce echipa *Guardian* „mătura rămășițele unui MacBook Pro".

Imaginea unui guvern care își trimite agenții la un ziar pentru a forța distrugerea computerelor acestuia este șocantă din start, fiind tipul de lucruri despre care occidentalilor li se spune că se întâmplă doar în locuri precum China, Iran și Rusia. Dar este, de asemenea, uluitor că un ziar venerabil a respectat voluntar, supus, astfel de ordine.

Dacă guvernul amenință cu închiderea ziarului, de ce să nu dezvălui amenințarea? Așa cum a spus Snowden când a auzit despre amenințare, „singurul răspuns corect este, haide, închide-ne!" Să te supui voluntar în secret înseamnă să permiți guvernului să își ascundă adevăratul caracter: o situație care oprește mișelește jurnaliștii de la a relata despre unul dintre cele mai semnificative subiecte în interesul public.

Mai rău, actul de a distruge materiale pentru care o sursă și-a riscat libertatea și chiar viața ca să le dezvăluie este cu totul la antiteza scopului jurnalismului.

Dincolo de necesitatea de a dezvălui un astfel de comportament despotic, merită fără îndoială o știre faptul că un guvern a intrat într-o redacție și a forțat un ziar să își distrugă informațiile. Dar *Guardian* se pare că a intenționat să rămână tăcut, demonstrând cât de precară este orice libertate a presei în Marea Britanie.

În orice caz, Gibson m-a asigurat că *Guardian* mai are o copie a arhivei în biroul din New York. Apoi mi-a dat o veste surprinzătoare: un alt set de documente se află la *New York Times*, dată de Alan Rusbridger redactorului-șef Jill Abramson, pentru a se asigura că ziarul are acces la fișiere chiar dacă justiţia britanică încearcă să forţeze *Guardian* US să distrugă copia sa.

Nici aceasta nu a fost o veste bună. Nu numai că *Guardian* a fost de acord, în secret, să distrugă propriile documente, dar fără să îl consulte sau măcar să ne avertizeze pe Snowden sau pe mine, le-a dat tocmai ziarului pe care Snowden îl exclusese pentru că nu avea încredere în relaţia strânsă și servilă pe care acesta o avea cu administraţia SUA.

Din perspectiva *Guardian*, acesta nu își permitea să fie sfidător în faţa ameninţărilor guvernului britanic, având în vedere absenţa protecţiei constituţionale, sutele de angajaţi pe care trebuia să îi protejeze și prestigiul ziarului vechi de un secol. Iar distrugerea computerelor era o variantă mai bună decât predarea arhivei către GCHQ. Dar eu am fost tulburat de conformarea lor faţă de cererile guvernului și, mai mult, de evidenta lor decizie de a nu relata despre acest lucru.

Cu toate acestea, atât înainte de distrugerea hard diskurilor sale, cât și după aceea, *Guardian* a rămas agresiv și îndrăzneţ în modul în care a publicat dezvăluirile lui Snowden – mai mult, cred eu, decât ar fi făcut orice alt ziar comparabil ca mărime și poziţie. În pofida tacticilor de intimidare ale autorităţilor, care s-au intensificat, redactorii au continuat să publice articole despre NSA și GCHQ unul după altul, și merită recunoaștere pentru acest lucru.

Dar Laura și Snowden au fost amândoi destul de furioși – pentru că *Guardian* s-a conformat unei astfel de intimidări guvernamentale și pentru că au rămas tăcuţi în legătură cu ce s-a întâmplat. Snowden a fost deosebit de furios că arhiva GCHQ a ajuns la *New York Times*. El a considerat acest lucru o încălcare a acordului său cu *Guardian* și a dorinţei sale ca doar jurnaliștii britanici să lucreze la documentele britanice și mai

ales ca publicației *New York Times* să nu i se dea documente. După cum s-a dovedit ulterior, reacţia Laurei a dus în cele din urmă la consecinţe dramatice.

De la începutul relatării noastre, relaţia Laurei cu *Guardian* a fost agitată, iar acum tensiunea a ieșit la iveală. În timp ce lucram împreună de o săptămână la Rio, Laura și cu mine am descoperit că o parte din arhiva NSA pe care Snowden mi-o dăduse în ziua în care mersese să se ascundă la Hong Kong (dar pe care nu avusese ocazia să i-o dea și Laurei) era coruptă. Laura nu a putut să rezolve problema la Rio, dar s-a gândit că poate va reuși când se va întoarce la Berlin.

O săptămână mai târziu, după ce s-a întors în capitala Germaniei, Laura mi-a transmis că arhiva este gata să îmi parvină. Am stabilit ca un angajat al *Guardian* să zboare la Berlin, să ia arhiva și apoi să mi-o aducă la Rio. Dar evident sub influenţa fricii după drama GCHQ, angajatul *Guardian* i-a spus Laurei că, în loc să îi dea arhiva lui personal, ar trebui să mi-o trimită prin FedEx.

Acest lucru a agitat-o și a înfuriat-o pe Laura așa cum nu o mai văzusem vreodată. „Nu vezi ce fac?“, m-a întrebat ea. „Vor să poată spune «Noi nu avem nimic de-a face cu transportarea acestor documente, Glenn și Laura și le-au transmis unul altuia»“. Ea a adăugat că folosirea FedEx pentru a transmite documente strict secrete în lume – și de a le trimite de la ea din Berlin mie la Rio, un indiciu clar către părţile interesate – era o încălcare gravă a securităţii operaţionale.

„Nu voi mai avea niciodată încredere în ei“, a declarat ea.

Dar încă aveam nevoie de acea arhivă. Aceasta conţinea documente vitale legate de subiecte la care lucram, precum și multe altele care așteptau să fie publicate.

Janine a insistat că problema a fost înţeleasă greșit, că angajatul a interpretat greșit comentariile supervizorului, că unii manageri de la Londra erau acum speriaţi de transportarea documentelor între Laura și mine. Nu era nici o problemă, a spus

ea. Cineva de la *Guardian* va zbura la Berlin să aducă arhiva chiar în acea zi.

Era prea târziu. „Nu voi da niciodată aceste documente ziarului *Guardian*“, a spus Laura. „Pur și simplu nu am încredere în ei“.

Mărimea și importanța arhivei au făcut-o pe Laura să nu vrea să le trimită electronic. Trebuiau livrate personal, de cineva în care ea avea încredere. Iar acel cineva era David care, atunci când a auzit despre problemă, s-a oferit imediat să meargă la Berlin. Amândoi am văzut aceasta drept soluţia perfectă. David a înţeles totul, Laura îl știa și avea încredere în el, și el oricum plănuia să o viziteze, ca să vorbească despre potenţiale proiecte noi. Janine a fost de acord cu ideea și a acceptat ca *Guardian* să acopere costurile de călătorie pentru David.

Biroul care se ocupă de deplasări la *Guardian* a cumpărat biletul pentru David la British Airways și i l-a trimis pe e-mail. Nu ne-am gândit la posibilitatea ca el să aibă vreo problemă. Jurnaliști de la *Guardian* care scriseseră articole despre arhiva lui Snowden, precum și angajații care transportaseră documentele dintr-o parte în alta zburaseră de pe aeroportul Heathrow de mai multe ori fără incidente. Chiar eu și Laura zburaserăm către Londra cu doar câteva săptămâni înainte. De ce să se gândească cineva că David – de departe o figură mult mai periferică – ar risca ceva?

David a plecat către Berlin duminică 11 august, urmând să se întoarcă după o săptămână cu arhiva de la Laura. Dar în dimineaţa în care urma să sosească, am fost trezit de un telefon foarte matinal. Vocea de la capătul celălalt al firului, care vorbea cu un puternic accent britanic, s-a identificat drept un „agent de securitate de pe aeroportul Heathrow“ și m-a întrebat dacă îl cunosc pe David Miranda. „Sunăm să vă informăm“, a continuat el, „că l-am reţinut pe domnul Miranda în baza legii privind terorismul din 2000, anexa 7“.

Nu am reacționat imediat la cuvântul „terorism“ – eram mai degrabă confuz. Prima întrebare pe care am adresat-o

a fost de cât timp este reţinut și când am auzit că sunt deja trei ore, am știut că nu este vorba despre o verificare standard privind imigraţia. Bărbatul a explicat că Marea Britanie are „dreptul legal“ de a-l reţine nouă ore în total, după care un tribunal poate extinde această durată. Sau îl pot aresta. „Încă nu știm ce vom face“, a spus agentul de securitate.

Atât Statele Unite, cât și Marea Britanie au arătat clar că nu există limite – etice, legale sau politice – pe care să le respecte atunci când pretind că acţionează în numele luptei împotriva „terorismului“. Acum, David era reţinut în baza unei legi privind terorismul. El nici măcar nu încercase să intre în Marea Britanie: se afla în aeroport în tranzit. Autorităţile britanice ajunseseră în ceea ce tehnic nici măcar nu este teritoriu britanic și îl reținuseră, iar acum invocau cel mai înfricoșător și întunecat motiv pentru a face acest lucru.

Avocaţii de la *Guardian* și diplomaţii brazilieni au trecut la treabă, încercând imediat să asigure eliberarea lui David. Nu eram îngrijorat de cum o să se descurce David în detenţie. O viaţă extrem de dificilă, întrucât crescuse într-un orfelinat dintr-una dintre cele mai sărace favele din Rio de Janeiro, îl făcuse foarte puternic, încăpăţânat și descurcăreţ. Știam că va înţelege exact ce se întâmplă și de ce, și nu mă îndoiam că le făcea anchetatorilor lui viaţa la fel de grea pe cât i-o făceau ei. Cu toate acestea, avocaţii *Guardian* au menţionat cât de rar se întâmplă să fie reţinut cineva atât de mult timp.

Căutând informaţii despre legea privind terorismul, am aflat că doar trei din 100 de persoane sunt oprite și cele mai multe interogatorii, peste 97%, durează mai puţin de o oră. Doar 0,06% sunt deţinute mai mult de șase ore. Se profila o probabilitate mare ca David să fie arestat la încheierea celor nouă ore de reţinere.

Scopul declarat al legii privind terorismul, așa cum sugerează și numele, este de a chestiona oamenii despre legăturile cu terorismul. Detenţia, pretinde guvernul britanic, este folosită pentru a „stabili dacă acea persoană este sau a fost implicată

în comandarea, pregătirea sau instigarea la acte de terorism“. Nu exista nici cea mai vagă justificare pentru reţinerea lui David în baza unei astfel de legi, decât dacă relatările mele erau echivalate cu terorismul, ceea ce părea să se întâmple.

Cu fiecare oră care trecea, situaţia părea din ce în ce mai sumbră. Tot ce știam era că diplomaţii brazilieni, precum și avocaţii de la *Guardian* încercau să îl localizeze pe David la aeroport și să obţină acces la el, dar totul fără succes. Însă cu doar două minute înainte de încheierea celor nouă ore, un mesaj de la Janine mi-a dat vestea pe care aveam nevoie să o aud, într-un singur cuvânt: „ELIBERAT“.

Reţinerea șocantă a lui David a fost condamnată imediat la nivel mondial ca o încercare mișelească de intimidare. O relatare a Reuters a confirmat că aceasta era într-adevăr intenţia guvernului britanic: „Un oficial american din domeniul securităţii a declarat pentru Reuters că unul dintre principalele scopuri ale... reţinerii și chestionării lui Miranda a fost să trimită un mesaj celor care au primit materialele lui Snowden, inclusiv *Guardian*, că guvernul britanic este serios în încercarea sa de a pune capăt scurgerilor de informaţii“[50].

Dar, așa cum le-am spus hoardelor de jurnaliști care s-au adunat la aeroportul din Rio, așteptând întoarcerea lui David, tacticile de intimidare ale Marii Britanii nu mă vor împiedica să continui să scriu. Mai mult, eram și mai impulsionat. Autorităţile britanice s-au arătat abuzive la extrem; singurul răspuns adecvat, în opinia mea, era exercitarea mai multor presiuni și solicitarea unei transparenţe și responsabilităţi mai mari. Aceasta este funcţia primară a jurnalismului. Atunci când am fost întrebat cum cred că va fi perceput episodul, am spus că eu cred că guvernul britanic va ajunge să regrete ce făcuse pentru că îl va face să pară represiv și abuziv.

O echipă a Reuters a distorsionat puternic și a tradus incorect comentariile mele – care au fost făcute în portugheză – spunând că răspunsul meu la ceea ce i-au făcut lui David va fi publicarea de documente despre Marea Britanie pe care

anterior decisesem să nu le dau la iveală. Având în vedere că este vorba despre o agenţie, această distorsiune a fost rapid transmisă în lumea întreagă.

În următoarele două zile, presa a relatat furios că promisesem să desfășor un „jurnalism de răzbunare". Era o denaturare absurdă: ceea ce am vrut să spun a fost că acest comportament abuziv al Marii Britanii m-a făcut doar mai hotărât să îmi continui activitatea. Dar așa cum am aflat de multe ori, să declari că ţi-au fost scoase comentariile din context nu face nimic pentru a opri mașinăria media.

Relatate greșit sau nu, reacţia la comentariile mele a fost grăitoare: Marea Britanie și Statele Unite se comportaseră ani la rând ca niște tirani, răspunzând oricărei provocări cu ameninţări și chiar mai rău. Autorităţile britanice obligaseră recent *Guardian* să își distrugă computerele și tocmai îl reţinuseră pe partenerul meu în baza legii privind terorismul. Avertizori de integritate au fost urmăriţi judiciar și jurnaliști au fost ameninţaţi cu închisoarea. Și totuși, chiar și percepţia unui răspuns puternic la o astfel de agresiune este întâmpinată cu o mare indignare din partea apologeţilor și a celor loiali statului: *Dumnezeule! Vorbește despre răzbunare!* Acceptarea docilă a intimidării exercitate de oficialităţi este văzută ca o obligaţie; sfidarea este condamnată ca un act de nesupunere.

După ce eu și David am scăpat în cele din urmă de camerele de luat vederi, am putut discuta. Mi-a spus că fusese sfidător pe parcursul celor nouă ore, dar a recunoscut că fusese speriat.

Fusese clar vizat: pasagerii zborului său au fost instruiţi să își prezinte pașapoartele agenţilor care așteptau la ieșirea din avion. Când l-au văzut pe al lui, a spus David, a fost reţinut în baza legii privind terorismul și „ameninţat din prima secundă până la ultima" că va merge la închisoare dacă nu va „coopera pe deplin". I-au luat tot echipamentul electronic, inclusiv telefonul mobil care conţinea fotografii personale, contactele sale și discuţiile cu prietenii, forţându-l să le spună parola

la telefon sub ameninţarea cu arestarea. „Mă simţeam de parcă îmi invadaseră toată viaţa, de parcă eram gol", a spus el.

David se tot gândea la ce făcuseră Statele Unite și Marea Britanie sub acoperirea luptei împotriva terorismului în ultimul deceniu. „Au răpit oameni, i-au închis fără să îi pună sub acuzare sau să le ofere dreptul la un avocat, i-au făcut să dispară, i-au dus la Guantanamo, i-au ucis", a spus el. „Nu este nimic mai înspăimântător decât ca aceste două guverne să îţi spună că ești un terorist", mi-a spus el – ceva ce nu li se va întâmpla majorităţii cetăţenilor americani sau britanici. „Îţi dai seama că îţi pot face orice."

Controversa privind reţinerea lui David a continuat săptămâni în șir. A fost principala știre în Brazilia timp de mai multe zile, iar populaţia braziliană a fost aproape unanim indignată. Politicienii britanici au cerut reformarea legii privind terorismul. Bineînţeles că a fost îmbucurător că oamenii au recunoscut actul Marii Britanii drept un abuz, ceea ce și era. În același timp însă, legea fusese un afront public mulţi ani – dar fiind în principal folosită împotriva musulmanilor, le-a păsat puţinor persoane. Nu era nevoie de reţinerea partenerului unui jurnalist occidental alb și renumit pentru a atrage atenţia asupra abuzului, dar aceasta s-a întâmplat.

Cum era de așteptat, s-a dovedit că guvernul britanic vorbise înainte cu Washingtonul despre reţinerea lui David. Întrebat într-o conferinţă de presă, un purtător de cuvânt al Casei Albe a spus: „A fost o avertizare... prin urmare era ceva despre care aveam indicii că este posibil să se întâmple"[51]. Casa Albă a refuzat să condamne reţinerea și a recunoscut că nu a făcut nimic pentru a o opri sau descuraja.

Majoritatea jurnaliștilor au înţeles cât de periculos era acest pas. „Jurnalismul nu este terorism"[52], a declarat indignată Rachel Maddow la emisiunea sa de la MSNBC, atacând esenţa subiectului. Dar nu toată lumea a simţit la fel. Jeffrey Toobin a lăudat guvernul britanic la o oră de maximă audienţă, echivalând comportamentul lui David cu cel al unui „cărăuș de

droguri“[53]. Toobin a adăugat că David ar trebui să fie mulţumit că nu fusese arestat și adus în faţa justiţiei.

Spectrul unei eventuale arestări a început să pară mai plauzibil atunci când guvernul britanic a anunţat că a început oficial o anchetă penală privind documentele pe care le transporta David. (La rândul său, David a iniţiat un proces împotriva autorităţilor britanice, afirmând că reţinerea sa a fost ilegală, pentru că nu a avut nimic de-a face cu scopul legii în baza căreia a fost reţinut: acela de a investiga legăturile unei persoane cu terorismul.) Nu te mai surprinde, așadar, că autorităţile sunt atât de impulsionate, atâta timp cât cei mai importanți jurnaliști compară relatarea esențială în interesul publicului cu ilegalitatea traficanţilor de droguri.

Cu puţin timp înainte de a muri, în 2005, David Halberstam, vestitul corespondent de război din Vietnam, a ţinut un discurs în faţa studenţilor de la Școala de Jurnalism Columbia. Cel mai măreţ moment al carierei sale[54], le-a spus el, a fost când generalii americani din Vietnam au ameninţat că vor cere redactorilor săi de la *New York Times* să nu îi mai permită să relateze despre război. Halberstam a spus că „înfuriase Washingtonul și Saigonul scriind articole pesimiste despre război“. Generalii l-au considerat „inamic“ de vreme ce le întrerupsese conferinţele de presă pentru a-i acuza de minciună.

Pentru Halberstam, faptul că înfuriase administraţia era un motiv de mândrie, adevăratul scop al jurnalismului. El știa că să fii jurnalist înseamnă să îţi asumi riscuri, să contești mai degrabă decât să te supui abuzurilor puterii.

Astăzi, pentru mulţi din această profesie, lauda din partea administraţiei pentru relatare „responsabilă“ – pentru acceptarea instrucţiunilor sale în legătură cu ce trebuie și ce nu trebuie publicat – este o insignă de onoare. Că aceasta este situația o dovedește faptul că jurnalismul critic a decăzut atât de mult în Statele Unite.

EPILOG

În prima conversaţie online pe care am avut-o cu Edward Snowden, el mi-a spus că se teme de un singur lucru în legătură cu ce se va întâmpla mai departe: că dezvăluirile sale ar putea fi primite cu apatie și indiferenţă, ceea ce ar fi însemnat că și-a distrus viaţa riscând închisoarea pentru nimic. Să spui că această teamă s-a spulberat înseamnă să minimalizezi prea dramatic cazul.

Într-adevăr, efectele acestei povești revelatoare au fost de departe mai mari, mai de durată și mai extinse decât am visat noi că ar fi posibil. Aceasta a concentrat atenţia lumii asupra pericolelor supravegherii omniprezente din partea statului și a secretului generalizat al guvernului. A generat prima dezbatere globală despre valoarea vieţii private individuale în epoca digitală și a determinat contestarea controlului hegemonic al Americii asupra internetului. A schimbat modul în care oamenii din lumea întreagă au văzut autenticitatea oricărei declaraţii făcute de oficialii SUA și a transformat relaţiile între ţări. A modificat radical opiniile despre adevăratul rol al jurnalismului în relaţia cu puterea guvernamentală. Iar în interiorul Statelor Unite, a generat o coaliţie diversă din punct de vedere ideologic și transpartinică, ale cărei presiuni au dus la o reformă semnificativă a supravegherii de către stat.

Un episod anume a subliniat schimbările profunde aduse de dezvăluirile lui Snowden. La doar câteva săptămâni după primul meu articol bazat pe dezvăluirile lui Snowden pentru *Guardian*, care a expus colectarea masivă de metadate de către NSA, doi membri ai Congresului au propus împreună un proiect de lege pentru ca acel program al NSA să nu mai primească fonduri. În mod remarcabil, cei doi iniţiatori ai proiectului au fost John Conyers, un liberal din Detroit care se află la

cel de-al douăzecilea mandat în Camera Reprezentanţilor, și Justin Amash, un conservator membru al mișcării Tea Party, aflat la al doilea mandat în Camera Reprezentanţilor. Este greu de imaginat doi membri mai diferiţi ai Congresului, dar iată-i uniţi de opoziţia lor faţă de spionajul intern al NSA. Iar propunerea lor a primit rapid zeci de susţineri din întregul spectru ideologic, de la cei mai liberali la cei mai conservatori – un eveniment cu adevărat rar la Washington.

Când legea a fost supusă votului, dezbaterea a fost televizată de C-SPAN și am umărit-o în timp ce discutam online cu Snowden, care se uita la C-SPAN de pe computerul din Moscova. Amândoi am fost uimiţi de ce am văzut. A fost, cred, pentru prima dată când a apreciat cu adevărat amploarea a ceea ce reușise el. Membrii Camerei Reprezentanţilor s-au ridicat unul după altul împotriva programului NSA, luând în derâdere ideea că o colectare a datelor apelurilor telefonice ale tuturor americanilor este necesară pentru oprirea terorismului. A fost de departe cea mai agresivă provocare la adresa statului invaziv, poliţienesc, care a apărut în Congres de la atacurile din 11 septembrie.

Până la dezvăluirile lui Snowden, era pur și simplu de neconceput ca un proiect desemnat să oprească finanţarea pentru un program major de securitate naţională să primească mai mult de o mână de voturi. Dar votul final pe baza proiectului de lege Conyers–Amash a șocat Washingtonul: a eșuat cu o diferenţă minusculă, de 205 la 217. Sprijinul a fost bipartizan, cu 111 democraţi și 94 de republicani care au votat în favoarea proiectului. Această ignorare a diviziunilor tradiţionale pe linie de partid a fost la fel de tulburătoare pentru Snowden și pentru mine ca și sprijinul substanţial pentru controlul NSA. Washingtonul se bazează pe un tribalism orb generat de războiul rigid între partide. Dacă arhitectura roșu versus albastru poate fi erodată și apoi depășită, există mult mai multă speranţă într-o politică bazată pe interesele actuale ale cetăţenilor.

În lunile care au urmat, pe măsură ce au fost publicate tot mai multe articole despre NSA în lume, mulţi experţi au anticipat că publicul își va pierde interesul pentru subiect. Dar de fapt interesul faţă de discuţiile privind supravegherea s-a intensificat, nu numai la nivel intern, ci și internaţional. Evenimentele dintr-o singură săptămână din decembrie 2013 – la peste șase luni după primul meu articol apărut în *Guardian* – ilustrează cât de mult au continuat să rezoneze dezvăluirile lui Snowden și cât de lipsită de susținere a devenit poziţia NSA.

Săptămâna a început cu o concluzie importantă[1] emisă de judecătorul federal american Richard Leon, că programul de colectare a metadatelor al NSA ar putea fi găsit vinovat de încălcarea celui de-al Patrulea Amendament al Constituţiei SUA, denunţându-l drept „aproape orwellian" ca proporţii. Așa cum am menţionat, juristul numit de Bush a adăugat explicit că administraţia nu a citat nici măcar un exemplu „în care analizele colectării masive de metadate a NSA" au oprit un atac terorist. După doar două zile, un comitet consultativ al președintelui Obama, format când a izbucnit pentru prima dată scandalul NSA, a publicat un raport de 308 pagini.[2] Raportul a respins în mod decisiv afirmaţiile NSA cu privire la importanţa spionajului său. „Analiza noastră sugerează că informaţia care a contribuit la anchetele teroriste prin folosirea secţiunii 215 [din Patriot Act] cu privire la metadatele telefonice nu a fost esenţială în prevenirea atacurilor", a scris comitetul, confirmând că în nici un moment rezultatul nu ar fi fost diferit „fără invocarea secţiunii 215 privind metadatele telefonice".

Între timp, în afara Statelor Unite se strângeau tot mai multe blamuri împotriva NSA. Adunarea Generală a ONU a votat unanim în favoarea unei rezoluţii – introduse de Germania și Brazilia – care afirma că intimitatea online este un drept uman fundamental, pe care un expert l-a caracterizat ca „un mesaj puternic pentru Statele Unite cum că este timpul să-și schimbe poziția și să pună capăt supravegherii NSA".[3] În aceeași zi, Brazilia a anunţat că nu va acorda un mult

așteptat contract în valoare de 4,5 miliarde de dolari pentru avioane de vânătoare companiei Boeing cu sediul în SUA, ci va cumpăra avioane de la compania suedeză Saab. Nemulţumirea Braziliei cu privire la spionarea de către NSA a liderilor săi, a companiilor și cetăţenilor săi a fost în mod clar un factor în această decizie surprinzătoare. „Problema NSA a întors lucrurile împotriva americanilor“[4], a declarat o sursă din cadrul guvernului brazilian pentru Reuters.

Nimic din toate acestea nu arată însă că bătălia a fost câștigată. Statul-securitate este incredibil de puternic, probabil chiar mai puternic decât cei mai înalţi oficiali aleși ai noștri, și se laudă cu numeroși supuși influenţi gata să îl apere cu orice preţ. Așa că nu este surprinzător că și acesta a înregistrat câteva victorii. La două săptămâni după decizia judecătorului Leon, un alt judecător federal, exploatând amintirile din 11 septembrie, a declarat programul NSA constituţional[5] într-un alt caz. Aliaţii europeni au renunţat la demonstraţiile lor iniţiale de furie, aliniindu-se supuși Statelor Unite, așa cum fac deseori. Sprijinul din partea publicului american a fost, de asemenea, inconsistent: sondajele arată că majoritatea americanilor, deși se opun programelor NSA dezvăluite de Snowden, vor totuși să îl vadă urmărit în justiţie pentru aceste dezvăluiri. Iar oficiali americani de rang înalt au început chiar să afirme că nu numai Snowden, ci și unii jurnaliști cu care a colaborat el, inclusiv eu, merită urmăriţi și închiși.

Cu toate acestea, susţinătorii NSA au fost în mod clar surprinși, iar argumentele lor împotriva reformei au fost tot mai slabe. Apărătorii supravegherii masive fără vreo suspiciune adeseori insistă, de exemplu, că un anumit grad de spionare este întotdeauna necesar. Dar este un argument ușor de demontat; nimeni nu contestă acest lucru. Alternativa la supravegherea în masă nu este eliminarea completă a supravegherii. Este, în schimb, o supraveghere ţintită, îndreptată doar împotriva acelora în privinţa cărora există dovezi substanţiale că sunt implicaţi în infracţiuni reale. O astfel de supraveghere

ţintită este mult mai probabil să împiedice comploturi teroriste decât actuala abordare „colectează tot“, care inundă agenţiile de informaţii cu atât de multe date încât analiștii nu le pot cerceta eficient. Și, spre deosebire de supravegherea în masă, respectă valorile constituţionale americane și preceptele de bază ale justiţiei occidentale.

Într-adevăr, ca urmare a scandalurilor privind abuzul de supraveghere descoperite de Comisia Church în anii 1970, exact acest principiu – că administraţia trebuie să ofere niște dovezi ale unei probabile infracţiuni sau al unui statut de agent străin înainte de a-i asculta conversaţiile personale – a dus la înfiinţarea tribunalului FISA. Din nefericire, tribunalul respectiv a fost transformat într-o mașină de ștampilat, fără să ofere o viziune juridică semnificativă a solicitărilor guvernamentale de supraveghere. Dar ideea esenţială a fost totuși exprimată și reprezintă un pas înainte. Convertirea tribunalului FISA într-un sistem judiciar real, mai degrabă decât o configuraţie cu un singur sens în care administraţia obţine ce vrea, ar fi o reformă pozitivă.

Este improbabil ca astfel de schimbări legislative interne să fie suficiente prin ele însele pentru rezolvarea problemei supravegherii, pentru că securitatea naţională cooptează atât de des entităţi care ar trebui să ofere supervizare. (Așa cum am văzut, de exemplu, comisiile pentru serviciile de informaţii din Congres sunt acum controlate integral.) Dar astfel de schimbări legislative pot măcar să sprijine principiul că supravegherea în masă fără discriminare nu își are locul într-o democraţie ghidată evident de garanţiile constituţionale ale vieţii private.

Alţi pași pot fi făcuţi pentru revendicarea intimităţii online și limitarea supravegherii din partea statului. Eforturi internaţionale – conduse în prezent de Germania și Brazilia – de construire a unei noi infrastructuri pentru internet astfel încât cea mai mare parte a traficului de internet să nu mai tranziteze Statele Unite ar putea să conducă la slăbirea controlului

american asupra internetului. Iar indivizii au, de asemenea, un rol de jucat în revendicarea propriei lor intimităţi online. Refuzând să folosească serviciile companiilor tehnologice care colaborează cu NSA și aliaţii săi, vor pune presiune pe aceste companii pentru a pune capăt unei astfel de colaborări și îi vor stimula pe competitorii lor să se dedice ei înșiși protecţiei vieţii private. Deja numeroase companii tehnologice europene își promovează serviciile de e-mail și chat ca o alternativă superioară la ofertele Google și Facebook, trâmbiţând faptul că ele nu oferă – și nu vor oferi – NSA datele utilizatorilor lor.

În plus, pentru a împiedica guvernele să se amestece în comunicaţiile personale și în folosirea internetului, toţi utilizatorii ar trebui să adopte instrumente de criptare și de navigare în mod anonim. Acest lucru este deosebit de important pentru persoanele care lucrează în domenii sensibile, precum jurnaliștii, avocaţii și activiștii pentru drepturile omului. Iar comunitatea tehnologică ar trebui să continue să elaboreze programe de criptare și de navigare anonimă mai eficiente și mai prietenoase pentru utilizatori.

Pe toate aceste fronturi, mai este mult de muncă. Dar la mai puţin de un an de când l-am întâlnit pentru prima dată pe Snowden în Hong Kong, fără îndoială că dezvăluirile lui au adus schimbări fundamentale și ireversibile în multe ţări și pe multe planuri. Și, dincolo de specificul reformei NSA, acţiunile lui Snowden au promovat în mod esențial cauza transparenţei guvernamentale și a reformei în general. El a creat un model pentru a-i inspira pe alţii, iar viitorii activiști îi vor călca probabil pe urme, perfecţionându-i metodele.

Administraţia Obama, care a adus mai multe urmăriri împotriva denunţătorilor decât toate celelalte președinţii laolaltă, a intenţionat să creeze un climat de teamă care să înăbușe orice încercare de denunţare. Dar Snowden a distrus acest șablon. El a reușit să rămână liber, în afara controlului Statelor Unite; și mai mult, el a refuzat să rămână ascuns, a luat atitudine și și-a declarat identitatea. Ca rezultat, imaginea lui publică

nu este cea a unui condamnat în uniformă portocalie și cătușe, ci a unei figuri independente și articulate care își poate expune opiniile, explicând ceea ce a făcut și de ce. Nu mai este posibil ca administrația SUA să distragă atenția de la mesaj doar prin demonizarea mesagerului. Este o lecție puternică aici pentru viitorii avertizori de integritate: să spui adevărul nu ar trebui să îți distrugă viața.

Iar pentru noi ceilalți, efectul inspirațional al lui Snowden nu este mai puțin profund. Destul de simplu, el a amintit fiecăruia despre extraordinara abilitate a ființei umane de a schimba lumea. Un om obișnuit în toate privințele – crescut de părinți care nu au avut avere sau putere, fără o diplomă de liceu, lucrând ca un obscur angajat al unei corporații gigantice – el, dintr-un simplu act de conștiință, a modificat cursul istoriei.

Chiar și cei mai implicați activiști sunt uneori tentați să cedeze în fața defetismului. Instituțiile actuale par prea puternice pentru a le provoca; doctrinele par mult prea înrădăcinate; există întotdeauna multe părți cu un interes legitim în menținerea statu-quo-ului. Dar ființa umană în mod colectiv, nu un număr mic de elite care lucrează în secret, este cea care poate decide în ce fel de lume vrem să trăim. Promovarea capacității umane de a raționa și de a lua decizii – acesta este scopul avertizării de integritate, al activismului, al jurnalismului politic. Și acest lucru se întâmplă acum, grație dezvăluirilor făcute de Edward Snowden.

Mulțumiri

În ultimii ani, eforturile guvernelor occidentale de a-și ascunde cele mai importante acţiuni de propriii lor cetăţeni au fost zădărnicite în mod repetat de o serie de dezvăluiri remarcabile făcute de avertizori de integritate curajoși. De-a lungul vremurilor, oameni care au lucrat în interiorul agenţiilor guvernamentale sau al instituţiilor militare din Statele Unite și din ţările aliate au decis că nu pot păstra tăcerea când descoperă nereguli grave. În schimb, ei vin și fac publice neregulile, uneori încălcând legea conștient, alteori nu, și întotdeauna cu un mare cost personal: riscându-și carierele, relaţiile personale și libertatea. Oricine trăiește într-o democraţie, oricine apreciază transparenţa și responsabilitatea le datorează acestor avertizori de integritate o mare recunoștinţă.

Lunga listă de predecesori care au constituit o sursă de inspirație pentru Edward Snowden începe cu cel care a publicat Documentele Pentagonului, Daniel Ellsberg, unul dintre eroii mei personali de multă vreme și acum prietenul și colegul meu, al cărui exemplu am încercat să îl urmez în toată activitatea pe care o desfășor. Alţi avertizori de integritate curajoși, care au îndurat persecuţia pentru a aduce la cunoștinţa lumii adevăruri vitale, sunt Chelsea Manning, Jesselyn Radack și Thomas Tamm, precum și foștii oficiali NSA Thomas Drake și Bill Binney. Ei au jucat de asemenea un rol esențial în acțiunea lui Snowden.

Aducerea la lumină a sistemului generalizat de supraveghere fără o bază de suspiciune construit în secret de Statele Unite și aliaţii lor a fost propriul act de conștiinţă autosacrificant al lui Snowden. Să vezi un tânăr de 29 de ani, de altfel un tip obișnuit, că riscă în mod conștient o viaţă în închisoare de dragul unui principiu, acţionând pentru apărarea drepturilor

elementare ale omului, a fost pur și simplu uimitor. Curajul lui Snowden și liniștea lui de nezdruncinat – adânc înrădăcinată în convingerea că face ceea ce trebuie – au inspirat toate relatările mele pe acest subiect și mă vor influența profund pentru tot restul vieţii.

Impactul acestui subiect ar fi fost imposibil fără prietena și partenera mea strălucită și extrem de curajoasă, jurnalista Laura Poitras. În pofida anilor de hărţuire din partea administraţiei americane pentru filmele pe care le-a făcut, ea nu a ezitat nici un moment să urmărească acest subiect în mod agresiv. Insistența ei asupra intimităţii personale, aversiunea ei față de lumina reflectoarelor au ascuns uneori faptul că a fost indispensabilă pentru activitatea pe care am putut-o desfășura. Dar experiența ei, geniul ei strategic, judecata și curajul ei au fost inima și sufletul întregii munci pe care am depus-o. Vorbim aproape zilnic și am luat fiecare decizie majoră în colaborare. Nu puteam cere un parteneriat mai reușit sau o prietenie care să mă impulsioneze și să mă inspire mai mult.

Așa cum eu și Laura știam, curajul lui Snowden a sfârșit prin a fi contagios. Numeroși jurnaliști au continuat subiectul fără teamă, inclusiv redactorii *Guardian* Janine Gibson, Stuart Millar și Alan Rusbridger, alături de câţiva reporteri ai ziarului, în frunte cu Ewen MacAskill. Snowden a reușit să rămână liber și prin urmare capabil să participe la dezbaterea pe care el a generat-o graţie sprijinului îndrăzneţ și indispensabil oferit de WikiLeaks și Sarah Harrison, unul dintre oficialii săi, care l-a ajutat să plece din Hong Kong și a rămas cu el timp de mai multe luni la Moscova riscându-și posibilitatea de a se întoarce în siguranţă în Marea Britanie, propria sa ţară.

Numeroși prieteni și colegi mi-au oferit sfaturi înţelepte și sprijin în multe situaţii dificile, printre aceștia numărându-se Ben Wizner și Jameel Jaffer de la ACLU; prietenul meu cel mai bun de-o viaţă, Norman Fleisher; unul dintre cei mai buni și mai curajoși jurnaliști de investigaţie, Jeremy Scahill; puternicul și abilul reporter brazilian Sonia Bridi de la Globo; directorul

executiv al Fundaţiei pentru Libertatea Presei Trevor Timm. Membrii familiei, care, adeseori îngrijoraţi de ce se întâmplă (așa cum doar membrii familiei pot fi), au rămas totuși susţinători statornici (cum numai membrii familiei pot fi), inclusiv părinţii mei, fratele meu Mark și cumnata mea Christine.

Aceasta nu a fost o carte ușor de scris, mai ales având în vedere circumstanţele, de aceea sunt cu adevărat recunoscător Metropolitan Books: lui Connor Guy pentru managementul său eficient; lui Grigory Tovbis pentru contribuţiile sale editoriale eficiente și experienţa sa tehnică; și mai ales lui Riva Hocherman, a cărei inteligenţă și standarde înalte au făcut-o cel mai bun redactor posibil pentru cartea de față. Aceasta este a doua carte consecutivă pe care am publicat-o cu Sara Bershtel, cu o minte remarcabil de înţeleaptă și creativă, și nu îmi pot imagina vreodată să vreau să scriu una fără ea. Agentul meu literar, Dan Conaway, a fost încă o dată o voce stabilă și chibzuită de-a lungul procesului. Profunde mulţumiri și lui Taylor Barnes pentru ajutorul ei esențial în conceperea acestei cărţi; talentele sale de cercetare și energia intelectuală nu lasă îndoială că are în față o carieră jurnalistică strălucită.

Ca întotdeauna, în centrul a tot ceea ce fac este partenerul meu de viaţă, soţul meu de nouă ani, sufletul meu pereche David Miranda. Chinul prin care a trecut pe parcursul relatării noastre a fost enervant și grotesc, dar avantajul a fost că lumea a văzut ce om extraordinar este. De fiecare dată, el mi-a insuflat îndrăzneală, mi-a susţinut hotărârea, mi-a ghidat alegerile, mi-a oferit perspective care mi-au clarificat lucrurile și a stat alături de mine, neclintit, cu sprijin necondiţionat și dragoste. Un astfel de parteneriat este neprețuit, pentru că alungă teama, distruge limitele și face totul posibil.

Note

Introducere

1. David Vincent, *The Culture of Secrecy in Britain, 1832–1998* (Oxford: Oxford University Press, 1998), 1–14
2. Peter Conolly-Smith, „«Reading Between the Lines»: The Bureau of Investigation, the United States Post Office, and Domestic Surveillance During World War I“, *Social Justice* 36, nr. 1 (2009): 7–24
3. Daniel Brückenhaus, „Every Stranger Must Be Suspected: Trust Relationships and the Surveillance of Anti-Colonialists in Early Twentieth-Century Western Europe“, *Geschichte und Gesellschaft* 36 (2010): 52366
4. Ben Elgin și Vernon Silver, „Syria Crackdown Gets Italy Firm's Aid with U.S.-Europe Spy Gear“, *Bloomberg News*, 3 noiembrie 2011
5. Steve Stecklow, Paul Sonne și Matt Bradley, „Mideast Uses Western Tools to Battle the Skype Rebellion“, *Wall Street Journal*, 1 iunie 2011
6. Margaret Coker și Paul Sonne, „Life Under the Gaze of Gadhafi's Spies“, *Wall Street Journal*, 14 decembrie 2011; Paul Sonne și Margaret Coker, „Firms Aided Libyan Spies“, *Wall Street Journal*, Ț30 august 2011
7. United States House of Representatives, „The internet in China: A Tool for Freedom or Suppression?“ Congresul 109, sesiunea a doua, 15 februarie 2006

1. Contactul

1. Glenn Greenwald, „U.S. Filmmaker Repeatedly Detained at Border“, Salon, 8 aprilie 2012
2. „U.S. Intelligence Planned to Destroy WikiLeaks“, WikiLeaks.org, 15 martie 2010, http://www.wikileaks.org/wiki/U.S._Intelligence_planned_to_ destroy_WikiLeaks,_18_Mar_2008

2. Zece zile în Hong Kong

1. *United States of America v. John Tomero et al.*, Defendants, S2 06 Crim. 0008, United States District Court (S.D. New York, 27 noiembrie 2006)
2. Christopher Drew și Scott Shane, „Résumé Shows Snowden Honed Hacking Skills“, *New York Times*, 4 iulie 2013
3. Howard Kurtz, „The Post on WMDs: An Inside Story“, *Washington Post*, 12 august 2004
4. James Risen și Eric Lichtblau, „Bush Lets U.S. Spy on Callers Without Courts“, *New York Times*, 16 decembrie 2005
5. Eric Lichtblau, „The Education of a 9/11 Reporter: The Inside Drama Behind the Times' Warrantless Wiretapping Story“, Slate, 26 martie 2008
6. Mark Sherman, „Government Obtains Wide AP Phone Records in Probe“, Associated Press, 13 mai 2013
7. Ann E. Marimow, „A Rare Peek into a Justice Department Leak Probe“, *Washington Post*, 19 mai 2013
8. „President Obama's Dragnet“, *New York Times*, 6 iunie 2013
9. Dan Roberts și Spencer Ackerman, „Anger Swells After NSA Phone Records Court Order Revelations“, *Guardian*, 6 iunie 2013
10. „ACLU Calls for End to Program, Disclosure of Program's Scope, Congressional Investigation“, 5 iunie 2013, https://www.aclu.org/national-security-technology-and-libertymassive-nsa-phone-data-mining-operation-revealed
11. Al Gore, postare pe Twitter, 5 iunie 2013, 18.39, https://twitter.com/algore/status/342455655057211393

3. Colectează tot

1. James Bamford, „Connecting the Dots on PRISM, Phone Surveillance, and the NSA's Massive Spy Center“, Wired, 12 iunie 2013, http://www.wired.com/2013/06/nsa-prism-verizon-surveillance/
2. Shane Harris, „The Cowboy of the NSA“, *Foreign Policy*, 9 septembrie 2013
3. Ellen Nakashima și Joby Warrick, „For NSA Chief, Terrorist Threat Drives Passion to «Collect It All», Observers Say“, *Washington Post*, 14 iulie 2013

4. Dana Priest și William M. Arkin, „A Hidden World, Growing Beyond Control“, *Washington Post*, 19 iulie 2010
5. William Binney, interviu cu Amy Goodman și Juan Gonzalez, *Democracy Now!*, 20 aprilie 2012
6. Siobhan Gorman și Jennifer Valentino-Devries, „New Details Show Broader NSA Surveillance Reach“, *Wall Street Journal*, 20 august 2013
7. Tim Shorrock, „Meet the Contractors Analyzing Your Private Data“, Salon, 10 iunie 2013
8. Gorman și Valentino-Devries, „New Details Show Broader NSA Surveillance Reach“
9. Robert O'Harrow Jr., Ellen Nakashima și Barton Gellman, „U.S., Company Officials: Internet Surveillance Does Not Indiscriminately Mine Data“, *Washington Post*, 9 iunie 2013
10. Elias Groll, „The PRISM Spin War Has Begun“, Foreign Policy, 7 iunie 2013
11. Claire Cain Miller, „Tech Companies Concede to Surveillance Program“, *New York Times*, 7 iunie 2013
12. Glenn Greenwald, Ewen MacAskill, Laura Poitras, Spencer Ackerman și Dominic Rushe, „Microsoft Handed the NSA Access to Encrypted Messages“, *Guardian*, 11 iulie 2013
13. David E. Sanger și Thom Shanker, „N.S.A. Devises Radio Pathway into Computers“, *New York Times*, 14 ianuarie 2014
14. Nick Hopkins și Julian Borger, „NSA Pays £100m in Secret Funding for GCHQ,“, *Guardian*, 1 august 2013
15. Ewen MacAskill, Julian Borger, Nick Hopkins, Nick Davies și James Ball, „GCHQ Taps Fibre-Optic Cables for Secret Access to World's Communications“, *Guardian*, 21 iunie 2013
16. James Ball, „US and UK Struck Secret Deal to Allow NSA to «Unmask» Britons' Personal Data“, *Guardian*, 20 noiembrie 2013
17. Interviul președintelui Barack Obama cu Charlie Rose, Public Broadcasting Service, 16 iunie 2013
18. Mike Rogers interviu cu Candy Crowley, CNN State of the Union, 16 iunie 2013
19. Interviu cu Mark Zuckerberg la Conferința TechCrunch Disrupt din San Francisco, 11 septembrie 2013
20. Jameel Jaffer, e-mail către Glenn Greenwald

21. Jack Balkin, „The Inspector General's Report and The Horse That Is Already Out of the Barn Door", Balkinization (blog), 11 iulie 2009, http://balkin.blogspot.com.br/2009/07/inspector-generals-report-and-horse.html
22. Matthew Keys, postare pe Twitter, 19 noiembrie 2013, 4.23, https://twitter.com/MatthewKeysLive/status/402774028898672640
23. Ryan Lizza, „State of Deception", New Yorker, 16 decembrie 2013
24. Dave Weigel, „New NSA Reform Bill Authorizes All the NSA Activity That Was Making You Angry", Slate, 1 noiembrie 2013
25. American Civil Liberties Union et al. v. James R. Clapper et al., 13-cv-03994, United States District Court (S.D. New York, 2013), https://www.aclu.org/files/pdfs/natsec/clapper/2013.08.26 ACLU PI Brief - Declaration - Felten.pdf
26. Barton Gellman și Ellen Nakashima, „U.S. Spy Agencies Mounted 231 Offensive Cyber-Operations in 2011, Documents Show", *Washington Pos*t, 30 august 2013.
27. James Glanz și Andrew W. Lehren, „N.S.A. Spied on Allies, Aid Groups and Businesses", *New York Times*, 20 decembrie 2013
28. Mike Rogers și C. A. Dutch Ruppersberger, *Investigative Report on the U.S. National Security Issues Posed by Chinese Telecommunications Companies Huawei and ZTE*, U.S. House of Representatives, Congresul 112, 8 octombrie 2012
29. Shane Harris și Isaac Stone Fish, „Accused of Cyberspying, Huawei Is «Exiting the U.S. Market»", Foreign Policy, 2 decembrie 2013
30. James Bamford, „The NSA Is Building the Country's Biggest Spy Center (Watch What You Say)", Wired, 15 martie, 2012

4. Răul produs de supraveghere

1. Eric Schmidt, interviu cu Maria Bartiromo, CNBC, 29 decembrie 2009
2. Mark Zuckerberg interviu cu Michael Arrington la TechCrunch în San Francisco, 9 ianuarie 2010
3. Mike German și Jay Stanley, Drastic Measures Required, American Civil Liberties Union, 3 iulie 2011
4. Priest și Arkin, „A Hidden World, Growing Beyond Control"
5. Carolyn Said, „Google Says CNET Went Too Far in Googling", *San Francisco Chronicle*, 9 august 2005

6. Chris Matyszczyk, „Zuckerberg Buys Four New Houses for, um, Privacy“, CNET, 11 octombrie 2013
7. Olmstead v. United States, United States Supreme Court, 277 U.S. 438 (1928)
8. Samuel D. Warren și Louis D. Brandeis, „The Right to Privacy“, *Harvard Law Review* 4, nr. 5 (15 decembrie 1890): 193–220
9. George Orwell, *Nineteen Eighty-Four* (New York: Alfred A. Knopf, 1992), 4–5. Prima ediție publicată de Secker and Warburg, 1949
10. Jeremy Bentham, *The Panopticon Writings*, ed. Miran Božovič (New York: Verso, 1995), 29. Prima ediție publicată în 1791
11. Michel Foucault, *Power: Essential Works of Foucault, 1954–1984*, vol. 3, ed. James D. Faubion, trad. Robert Hurley (New York: New Press, 2000), 70
12. Ian Traynor și Paul Lewis, „Merkel Compared NSA to Stasi in Heated Encounter with Obama“, *Guardian*, 17 decembrie 2013
13. Larry Siems, „A Blacklisted Screenwriter on American Surveillance“ (Interviu al lui Siems cu Walter Bernstein), PEN America, 30 august 2013
14. „Chilling Effects: NSA Surveillance Drives U.S. Writers to Self-Censor“, PEN America, 12 noiembrie 2013, 3
15. Pierrick Bourrat, Nicolas Baumard și Ryan McKay, „Surveillance Cues Enhance Moral Condemnation“, *Evolutionary Psychology* 9, nr. 2 (2011): 193–199
16. Gregory L. White și Philip G. Zimbardo, *The Chilling Effects of Surveillance: Deindividuation and Reactance*, Office of Naval Research, mai 1975
17. Mikael Priks, „Do Surveillance Cameras Affect Unruly Behavior? A Close Look at Grandstands“ (working paper no. 2289, Center for Economic Studies of the Leibniz Institute for Economic Research [CESifo], Universitatea din München, aprilie 2008)
18. Kristen Munger și Shelby J. Harris, „Effects of an Observer on Handwashing in a Public Restroom“, Perceptual and Motor Skills 69 (1989): 733–734; D. M. Pedersen, S. Keithly și K. Brady, „Effects of an Observer on Conformity to Handwashing Norm“, *Perceptual and Motor Skills* 62, nr. 1 (martie 1986): 169–170
19. C. Mancini, Y. Rogers, K. Thomas, et al., „In the Best Families: Tracking and Relationships“, Proceedings of the 29th International Conference on Human Factors in Computing Systems (New York: ACM Press, 2011), 2419–2428

20. Antti Oulasvirta, Aurora Pihlajamaa, Jukka Perkiö, et al., „Long-Term Effects of Ubiquitous Surveillance in the Home“, Proceedings of the 2012 ACM Conference on Ubiquitous Computing (New York: ACM Press, 2012), 41–50
21. Barton Gellman, „Digital Privacy: If You’ve Done Nothing Wrong, Do You Have ‘Nothing to Hide’?“, Time, 3 august 2010
22. „The New Line on Wiretapping“, Time, 25 iulie 1969
23. Eric Lichtblau și James Risen, „Defense Lawyers in Terror Cases Plan Challenges over Spy Efforts“, *New York Times*, 28 decembrie 2005
24. Interviul președintelui Barack Obama cu Jay Leno, The Tonight Show, NBC, difuzat în 7 august 2013
25. Brandenburg v. Ohio, United States Supreme Court, 395 U.S. 444 (1969)
26. United States Senate, *Final Report of the Select Committee to Study Governmental Operations with Respect to Intelligence Activities*, 26 april 1976
27. COINTELPRO memo explained Betty Medsger, *The Burglary: The Discovery of J. Edgar Hoover’s Secret FBI* (New York: Alfred A. Knopf, 2014), 160
28. *1971*, regizor Johanna Hamilton, Maximum Pictures, 201
29. Citat în Medsger, *The Burglary*, 184
30. „Documents Shed New Light on Pentagon Surveillance of Peace Activists“, *American Civil Liberties Union News Release*, 12 octombrie 2006
31. Muslim American Civil Liberties Coalition (MACLC), Creating Law Enforcement Accountability and Responsibility (CLEAR) Project, și Asian American Legal Defense and Education Fund (AALDEF), *Mapping Muslims: NYPD Spying and Its Impact on American Muslims*, CLEAR Project, City University of New York Law School, 11 martie 2013
32. Glenn Greenwald, Ryan Gallagher și Ryan Grim, „Top-Secret Document Reveals NSA Spied on Porn Habits as Part of Plan to Discredit «Radicalizers»“, *Huffington Post*, 26 noiembrie, 2013
33. Mark Schone, Richard Esposito, Matthew Cole și Glenn Greenwald, „War on Anonymous: British Spies Attacked Hackers, Snowden Docs Show“, NBC, 4 februarie 2014

34. Cass R. Sunstein și Adrian Vermeule, „Conspiracy Theories“ (Harvard University Law School Public Law and Legal Theory Research Paper Series, 15 ianuarie 2008)
35. Lawrence O'Donnell interviu cu Glenn Greenwald, *The Last Word with Lawrence O'Donnell*, MSNBC, 10 iunie, 2013
36. Hendrik Hertzberg, „Snoop Scoops“, *New Yorker,* 24 iunie 2013
37. Ruth Marcus, „Edward Snowden, the Insufferable Whistleblower“, Washington Post, 31 decembrie 2013
38. „Few See Adequate Limits on NSA Surveillance Programs“, Pew Research Center for the People and the Press news release, 26 iulie 2013
39. „Surveillance in America: Washington Post Poll: Government and Corporate Surveillance Draw Wide Concern“, Washington Post, 22 decembrie 2013
40. Orin Kerr, „Liberals and Conservatives Switch Positions on NSA Surveillance“, *The Volokh Conspiracy* (blog), 24 decembrie 2013
41. Interviu cu senatorul Joe Biden, *The Early Show*, CBS, 12 mai, 2006
42. Benjamin Wallace-Wells, „Patriot Act: The Kitchen Sink Approach to National Security“, *New York*, 27 august 2011
43. Interviu cu senatorul Frank Church, Meet the Press, NBC, 17 august 1975
44. James Bamford, „The Agency That Could Be Big Brother“, *New York Times*, 25 decembrie, 2005
45. Hertzberg, „Snoop Scoops“
46. Greg Miller și Ellen Nakashima, „Officials' Defenses of NSA Phone Program May Be Unraveling“, *Washington Post*, 19 decembrie 2013
47. *Liberty and Security in a Changing World: Report and Recommendations of The President's Review Group on Intelligence and Communications Technologies*, Review Group on Intelligence and Communications Technologies, 12 decembrie 2013 (publicat în 18 decembrie 2013)
48. Miller și Nakashima, „Officials' Defenses of NSA Phone Program May Be Unraveling“
49. Ron Wyden, Mark Udall și Martin Heinrich, „End the N.S.A Dragnet Now“, *New York Times*, 25 noiembrie 2013
50. Peter Bergen, David Sterman, Emily Schneider și Bailey Cahall, „Do NSA's Bulk Surveillance Programs Stop Terrorists?“, New America Foundation, 13 ianuarie 2014

51. Ellen Nakashima, „NSA Phone Record Collection Does Little to Prevent Terrorist Attacks, Group Says“, *Washington Post*, 12 ianuarie 2014
52. Generalul Keith Alexander, mărturie în fața Comisiei din Camera Reprezentanților, 18 iunie 2013
53. Peter Bergen, „Would NSA Surveillance Have Stopped 9/11 Plot?“, CNN, 30 decembrie 2013
54. Lawrence Wright, „The Al Qaeda Switchboard“, *New Yorker*, 13 ianuarie 2014
55. Rush Holt, „When Big Brother Meets Big Data“, *Huffington Post*, 27 iunie 2013
56. Bruce Schneier, „How the NSA Threatens National Security“, *Atlantic*, 6 ianuarie 2014
57. John Mueller citat în Kim Murphy, „Is Homeland Security Spending Paying Off?“, *Los Angeles Times*, 28 august 2011
58. Warren P. Strobel, „Terrorism in 2009“, McClatchy *Nukes and Spooks* (blog), 5 august 2010
59. Stephen M. Walt, „What Terrorist Threat?“, *Foreign Policy*, 13 august 2012
60. Senatorul Pat Roberts, remarcă din timpul audierii din Senat pentru confirmarea generalui Michael Hayden ca director al CIA, 18 mai 2006
61. Jonathan Allen, „Civil Liberties Don't Matter Much «After You're Dead», Cornyn Says on Spy Case“, Hill, 20 decembrie 2005
62. Rush Limbaugh, *The Rush Limbaugh Show*, 19 decembrie 2005.
63. Bentham, *The Panopticon Writings*, 43

5. A patra putere

1. Noam Cohen și Leslie Kaufman, „Blogger, with Focus on Surveillance, Is at Center of a Debate“, *New York Times*, 6 iunie 2013
2. Margaret Sullivan, „Who's a Journalist?: A Question with Many Facets and One Sure Answer“, *New York Times*, 29 iunie 2013
3. Charlie Savage, „Holder Tightens Rules on Getting Reporters' Data“, *New York Times*, 12 iulie 2013
4. Ann E. Marimow, „Justice Department's Scrutiny of Fox News reporter James Rosen in Leak Case Draws Fire“, *Washington Post*, 20 mai 2013

5. Olivier Knox, „Obama Administration Spied on Fox News Reporter James Rosen: Report“, *Yahoo! News*, 20 mai 2013
6. Charlie Savage, „U.S. Gathered Personal Data on Times Reporter in Case Against Ex-C.I.A. Agent“, *New York Times*, 25 februarie 2011
7. Martha T. Moore și Aamer Madhani, „Is Obama at War with Journalists?“, USA Today, 27 mai 2013
8. Molly Redden, „Is the ‘Chilling Effect’ Real?: National-Security Reporters on the Impact of Federal Scrutiny“, *New Republic*, 15 mai 2013
9. Leonard Downie Jr., „The Obama Administration and the Press: Leak Investigations and Surveillance in Post-9/11 America“, Committee to Protect Journalists, 10 octombrie 2013
10. Mark Landler, „Obama, in Nod to Press, Orders Reviews of Inquiries“, *New York Times*, 23 mai 2013
11. Tom McCarthy, „Eric Holder: Justice Department Will Not Prosecute Reporters Doing Their Job“, *Guardian*, 6 iunie 2013
12. Interviul congresmenului Peter King cu Anderson Cooper, Anderson Cooper 360 Degrees, CNN, 11 iunie 2013
13. Interviul congresmenului Peter King cu Megyn Kelly, *America Live*, Fox News, 12 iunie 2013
14. Marc A. Thiessen, „Yes, Publishing NSA Secrets Is a Crime“, *Washington Post*, 17 iunie 2013
15. Alan Dershowitz, interviu cu Piers Morgan, Piers Morgan Live, CNN, 24 iunie 2013
16. Michael Hayden, „Ex-CIA Chief: What Edward Snowden Did“, CNN, 19 iulie 2013
17. Dana Milbank, „In Ex-Aide’s Testimony, a Spin Through VP’s PR“, *Washington Post*, 26 ianuarie 2007
18. Glenn Greenwald, interviu cu David Gregory, Meet the Press, NBC, 23 iunie 2013
19. Reliable Sources, CNN, 30 iunie 2013
20. Walter Pincus, „Questions for Snowden“, *Washington Post*, 8 iulie 2013
21. Andrew Ross Sorkin, *Squawk Box*, CNBC, 24 iunie 2013
22. HuffPost Media, postare pe Twitter, 23 iunie 2013, 7.59, https://twitter.com/HuffPostMedia/status/348817574101 909507
23. Toby Harnden, postare pe Twitter, 23 iunie 2013, 8.33, https://twitter.com/tobyharnden/status/348826074043 539457

24. Scrisoare de la Alan Grayson către Eric Holder, 10 octombrie 2013
25. Keith Alexander, „I Spy, No Lie", interviu cu Armed with Science: *The Official U.S. Defense Department Science Blog* (blog), 24 octombie 2013
26. Josh Gerstein, „Intelligence Chairman Accuses Glenn Greenwald of Illegally Selling Stolen Material", *Politico*, 4 februarie 2014
27. Paul Calandra, declarație în Camera Comunelor, Canada, 14 februarie 2014
28. Bob Schieffer, „Edward Snowden Is No Hero", CBS News, 16 iunie 2013
29. Jeffrey Toobin, „Edward Snowden Is No Hero", *New Yorker*, 10 iunie 2013
30. Richard Cohen, „The NSA Is Doing What Google Does", *Washington Post*, 10 iunie 2013
31. David Brooks, „The Solitary Leaker", *New York Times*, 10 iunie 2013
32. Roger Simon, „The Slacker Who Came In from the Cold", *Politico*, 11 iunie 2013
33. Aaron Blake, „DNC Chair Debbie Wasserman Schultz: Snowden Is a Coward", *Washington Post*, 11 iunie 2013
34. Matt Mackowiak, postare pe Twitter, 9 iunie 2013, 13.07, https://twitter.com/MattMackowiak/status/34382157211 4624514
35. Jane Perlez și Keith Bradsher, „China Said to Have Made Call to Let Leaker Depart", *New York Times*, 23 iunie 2013
36. Glenn Greenwald, „Snowden: I Never Gave Any Information to Chinese or Russian Governments", *Guardian*, 10 iulie 2013
37. Margaret Sullivan, „How Acceptable Was Anonymous Speculation About Snowden's Laptops?", *New York Times*, 11 iulie 2013
38. Evan Osnos, „Why China Let Snowden Go", *New Yorker*, 24 iunie 2013
39. John F. Burns, „WikiLeaks Founder on the Run, Trailed by Notoriety", *New York Times*, 23 octombrie 2010
40. Bill Keller, „Dealing with Assange and the WikiLeaks Secrets", *New York Times*, 26 ianuarie 2011
41. Peter Ludlow, „The Banality of Systemic Evil", *New York Times*, 15 septembrie 2013
42. Glenn Greenwald, interviu cu David Gregory, Meet the Press, NBC, 23 iunie 2013

43. Jack Shafer, „From Tom Paine to Glenn Greenwald, We Need Partisan Journalism“, Reuters, 16 iulie 2013
44. Byron Calame, „Behind the Eavesdropping Story, a Loud Silence“, New York Times, 1 ianuarie 2006
45. Brian Ross și Vic Walter, „Whistle-blower Had to Fight NSA, LA Times, to Tell Story“, ABC News, 6 martie 2007
46. Margaret Sullivan, „Sources With Secrets Find New Outlets for Sharing“, *New York Times*, 16 iunie 2013
47. Bill Keller interviu la BBC News, 29 noiembrie 2010
48. Jack Goldsmith, „The Patriotism of the American Media“, *Lawfare* (blog), 28 februarie 2011
49. Lisa O'Carroll, „Seymour Hersh on Obama, NSA and the «Pathetic» American Media“, *Guardian*, 27 septembrie 2013
50. Mark Hosenball, „Britain Forced Guardian to Destroy Copy of Snowden Material“, Reuters, 19 august 2013
51. Josh Earnest, întâlnire cu presa la Casa Albă, 19 august 2013
52. Rachel Maddow, *The Rachel Maddow Show*, MSNBC, 20 august 2013
53. Jeffrey Toobin cu Anderson Cooper, *Anderson Cooper 360 Degrees*, CNN, 20 august 2013
54. David Halberstam, discurs ținut la Columbia Journalism School, 18 mai 2005

Epilog

1. Spencer Ackerman și Dan Roberts, „NSA Phone Surveillance Program Likely Unconstitutional, Federal Judge Rules“, *Guardian*, 16 decembrie 2013
2. *Liberty and Security in a Changing World*, Review Group on Intelligence and Communications Technologies
3. Edith M. Lederer, „UN Votes to Protect Privacy in Digital Age“, Associated Press, 18 decembrie 2013
4. Alonso Soto și Brian Winter, „Saab Wins Brazil Jet Deal After NSA Spying Sours Boeing Bid“, Reuters, 19 decembrie 2013
5. Adam Liptak și Michael S. Schmidt, „Judge Upholds NSA's Bulk Collection of Data on Calls“, *New York Times*, 27 decembrie 2013

INDICE